

MusLinc - Privacy Policy

Effective Date: Last Updated: 30 July 2026

Introduction

MusLinc Ltd (“MusLinc”, “we”, “us” or “our”) is committed to protecting your privacy. This Privacy Policy explains how we collect, use, share, and safeguard your personal information when you use the MusLinc mobile application, website, and any related services (collectively, the “Services”). It also outlines your rights under UK data protection laws and how we comply with UK GDPR, the Data Protection Act 2018, and other relevant regulations. We aim to use clear, friendly language while ensuring legal compliance, so please read this policy carefully. By using MusLinc, you agree to the collection and use of information in accordance with this Privacy Policy and our Terms & Conditions.

Who We Are

MusLinc Ltd is a company registered in England and Wales (company number: 16740431) with its registered office at MusLinc 16740431, 60 Tottenham Court Road, Suite 6621a, Fitzrovia, London, United Kingdom, W1T 2EW. For the purposes of data protection law, MusLinc Ltd is the “data controller” of your personal information. If you have any questions about this Privacy Policy or your data, you can contact us at privacy@Muslinc.com or by post at MusLinc 16740431, 60 Tottenham Court Road, 6621a, Fitzrovia, London, United Kingdom, W1T 2EW. We have appointed a Data Protection Officer (DPO) who can be reached via the email address privacy@Muslinc.com.

1. Information We Collect

We collect various types of information about you to provide and improve our Services, to keep our community safe, and to comply with legal obligations. This includes:

- **Information You Provide Directly:** When you create an account or profile, you give us information such as your name, email address, phone number, date of birth, gender, preferences, photos, and a short bio. You may also provide information about your interests, location (e.g. city or region), and other profile details when filling out your profile or updating it. Any information you share on your profile will be visible to other users of the app. Please do not include personal contact details (like your last name, home address, phone number, or email) in your public profile to protect your privacy. If you choose to disclose personal information to other users in private communications, you do so at your own risk. We encourage you to exercise the same caution in sharing details with people you meet on MusLinc as you would elsewhere.
- **Sensitive Personal Data (Special Category Data):** In some cases, you may provide information that is considered sensitive under data protection law. This can include data about your racial or ethnic origin, religious beliefs, health, or biometric data (for example, a facial image for verification purposes). Any such information is entirely optional and provided by you at your discretion. For instance, because MusLinc is a community focused on connecting like-minded individuals, you may choose to share your religion or cultural background on your profile. We treat this as “special category” personal data and apply additional protections. By providing this information, you consent to our processing of it for the purpose of delivering the Services (e.g. showing it on your profile). We will never use sensitive data for targeted advertising or share it without your explicit consent, except as described in this policy. Stronger legal safeguards apply to sensitive information such as race, ethnic background, religious beliefs, health, genetics or biometric identifiers, and we comply with those requirements.
- **Selfies, Photos and Verification Data:** As part of our commitment to a safe, authentic community, we may ask you to complete a Selfie Verification during registration or later. This means you might provide us a photo of yourself (“selfie”) within the app. We use this selfie strictly to verify that you are a real person and that your profile photos match your real appearance. We never share your selfie with other users or the public. In some cases, we use a trusted third-party identity verification service (our “Verification Provider— Amazon Web Services -AWS (“aws.amazon.com”) to help confirm your identity. For example, we might utilize facial recognition technology to compare your selfie with your profile picture to ensure they appear to be the same person. The Verification Provider (AWS) may process your selfie to create a unique biometric identifier (a facial template) and determine a match score. Important: MusLinc does not receive or store any biometric identifier data; such data is generated and used by the Verification Provider (solely for the verification process and is promptly deleted after completing the check. We only receive confirmation of whether you passed the verification and possibly a verified status (like a badge on your profile). In the event a selfie or document you submit is identified as fraudulent or not matching (for example, a photo of someone else), we may retain that information or pass it to AWS to improve fraud detection algorithms. We will inform you if additional steps or re-submission are required. All selfie/ID verification data is handled with care and not used for any purpose other than fraud prevention, security, and verifying your identity.
- **Profile Content and User-Generated Content:** When using MusLinc, you may provide information in other ways – for example, if you fill out optional profile sections (like interests, personal descriptions), answer app questions or prompts, or

upload additional photos/videos, voice notes, or other media. If the Service offers features like posting status updates, participating in forums or public chats, or answering icebreaker questions, the content you provide (including any personal information about yourself or others within it) will be processed by us and visible to others according to the privacy settings of that feature. Please only share content that you are comfortable being seen by others and that complies with our Acceptable Use Policy.

- **Communications and Messages:** We collect content of communications between you and other users as part of providing the Service. For instance, when you send and receive messages or voice/video calls through the app, those communications are transmitted through our systems and may be stored, at least temporarily. Private chats are generally only visible to the participants; however, MusLinc reserves the right to review and moderate communications if they are reported for violating our policies or to ensure the safety of our users. We may use automated tools (and limited human review where necessary) to scan messages for red flags (like keywords related to scams or abuse) in order to detect and prevent harmful behaviour, as permitted by law.
- **Usage Data:** We automatically collect certain information when you use the Services. This includes:
 - **Log and Device Data:** Details about your logins and usage of the app, such as the dates and times of logins, features used, clicks and pages viewed, referring webpage, and crashes or error reports. It also includes technical information about your device and internet connection, like device model, operating system, unique device identifiers, browser type (for web access), IP address, and version of our app. This data helps us ensure compatibility with your device, fix bugs, and improve performance.
 - **Location Information:** With your permission, we collect approximate location data of your device. For example, we may use GPS data, Wi-Fi access points, cell tower information, and IP address to determine your general location. MusLinc uses location data to provide location-based matching and features – for instance, to show you relevant profiles near you or to verify that profile locations are genuine (to maintain trust in our community). We may also verify your location consistency to prevent fake profiles (e.g. checking that your stated city matches your device location). We do not track your precise real-time movements in the background, but we may update your last known general location when you actively use the app (e.g. city or region). You can control location sharing via your device settings, and you may still use the app with location turned off, though some features (like seeing nearby matches or location verification) might be limited.
 - **Cookies and Similar Technologies:** When you visit our website or use the app, we (and our third-party analytics or advertising partners) may use cookies, pixels, SDKs, and similar tracking technologies to collect information about your usage and preferences. This can include remembering your login session, understanding how you navigate the Service, and tailoring content or advertisements (if any). Our Cookie Policy provides more details on these technologies and your choices. Generally, these tools help us improve and secure our Services, remembering your preferences and recognizing you across sessions. For example, we may use cookies to keep you logged in, to save your app settings, or to measure traffic and usage patterns.
 - **Information from Third-Party Sources:** If you create your MusLinc account by connecting through a third-party account (such as Google, Apple, or Facebook), we receive information from that account – specifically, the email address associated with it and possibly your name and profile photo, as needed to set up your account. This is used to streamline registration and verify your identity. We do not post anything to those third-party accounts without your permission. Additionally, if you choose to integrate or share content through third-party social media (for example, sharing your MusLinc profile or moments to another platform), those platforms may send us information as required for that integration. We also may receive information from partners or service providers to supplement or validate our data – for example, age or ID verification services might confirm your age or identity, payment processors may provide billing info (like confirmation of subscription payment), and analytics providers might give us demographic or preference insights. Any such data is either information you have already made public or provided consent for the third party to share. We treat combined information in accordance with this Privacy Policy.

We do not knowingly collect personal information from anyone under 18 years old. MusLinc is strictly for adults only, and we take steps to prevent underage users from joining (including age-verification checks). If you are under 18, please do not use our Services or provide any personal data. If we learn that an under-18 user is on our platform, we will take immediate action to remove the account and any associated information. If you believe we might have data from or about a minor, please contact us so we can investigate and delete it.

2. How We Use Your Information

We use the personal information we collect for the following purposes:

- **To Provide and Operate the Services:** First and foremost, we process your data to create and manage your account, and to allow you to use MusLinc's features. This includes displaying your profile to other users, introducing you to potential matches, and enabling you to connect and communicate with others (e.g., by showing your profile in the

discovery or search features, and delivering your chat messages). It also includes using your data to operate core app functions such as authentication (logging you in), applying your preferences (e.g. search filters), and matching algorithms (to suggest compatible profiles). Our matching system may use information like your profile details and activity to recommend other users that you might be interested in – this involves algorithmic processing of your data, but does not amount to an automated decision that has legal or significant effects; rather, it's a personalized suggestion feature, and you always have the choice of whom to connect with. We may periodically highlight certain users or content (for example, showing you new members in your area or suggesting profiles with common interests).

- **To Maintain a Safe and Respectful Community (Safety and Moderation):** Keeping MusLinc safe is a top priority. We use personal data to prevent and combat fraud, harassment, and other violations of our Terms or policies. For example, we will use data such as profile content, chat messages, and user reports to detect fake profiles, spam, or inappropriate content. We employ a combination of automated systems and human moderators to review content that is flagged or reported, and to take appropriate action (which may include content removal or account suspension). We also use personal identifiers like device IDs and IP addresses to help identify and block malicious actors (for instance, to enforce bans or prevent users who were removed from returning with new accounts). If necessary, we may use information about a user's device or network to enforce technical measures against prohibited automated tools (like bots or scrapers). Additionally, we may use and disclose personal data where needed to investigate and address unlawful activities – for example, to look into claims of fraud or to respond to legal requests (see "Legal Obligations" below). We want MusLinc to be a place where everyone feels safe and respected, so data about any reports you make (or that others make about you) will be stored so we can track recurring issues and outcomes. Note: We do not listen to or store your calls – those are typically peer-to-peer or ephemeral. However, we may log that a call occurred (time, user IDs) for safety and support purposes.

- **Verification and Trust Features:** We use the information you provide to verify accounts and build trust in the community. This includes using your selfie verification data to grant verified badges and performing checks on profile info (like ensuring your photos match your selfie, or your location data matches your stated location). We might also use identity document verification in the future (e.g., asking for a photo of your ID) if we introduce an ID-verify feature – such data would be used solely to confirm your identity or age and then discarded or stored securely in accordance with law. If you opt to verify your profile or identity, we will show other users an indicator (badge) that you have been verified. However, as noted, verification processes are on a best-efforts basis and cannot guarantee that a user is who they claim or that they have no bad intentions. We will use verification outcomes to block or remove accounts that fail checks (for instance, if someone refuses required age verification or is found using someone else's photos). Our verification provider is AWS – please check their details [here](https://aws.amazon.com) aws.amazon.com.

- **To Personalize Your Experience:** We want to make your experience on MusLinc engaging. We may use your information to customize the content you see, such as suggesting relevant profiles, showing local events or content if we have any, or ordering the profiles you see in a way intended to highlight likely matches. We also might remember the last section you visited or features you use often to streamline your interactions. If you have given us permission, we might use certain data to personalize any marketing or communications we send you (for example, highlighting new features that align with your usage patterns).

- **To Communicate with You:** We will use your contact information (email address and/or in-app notifications) to send you important account or service updates. These include confirmations of actions (like successful sign-ups or purchases), notifications of matches or messages (so you don't miss a chat), and changes to our Terms or policies. We may also send you promotional communications about new MusLinc features, events, or offers, but you will have the ability to opt out of marketing emails or notifications if you wish. We will keep our communications respectful and not excessive. If you contact us for support, we will use your name and email (and any other info you provide) to respond to your inquiry and resolve any issues. We may keep records of your communications with us (such as support emails or chat with our team) to better assist you in the future and improve our support services.

- **For Payments and Transactions:** If you choose to purchase a premium subscription or any in-app feature (such as profile boosts or other paid services), we will use the personal and payment information you provide to process those transactions. We do not directly collect or store full payment card details; payments are handled by third-party payment processors (e.g., Stripe, Apple App Store, Google Play) who may collect your payment data securely. We receive confirmation of your purchase and basic details like the type of subscription or product and the date/time of purchase. We use this to activate your premium features, manage your subscription (such as renewing it if it's an auto-renewing plan), and handle any billing issues or inquiries. We may also use purchase history to provide customer support (e.g., refund requests) or to inform you of related offers (for instance, letting you know when a promotional upgrade is available, if you have given marketing consent). All payments are subject to our Terms & Conditions and potentially the app store's terms, and we process your data consistent with those.

- **Analytics and Service Improvement:** We want to continually make Muslinc better. To that end, we use analytics tools (which may involve cookies and similar technologies on our site/app) to collect data about how users engage with our

Service. This information includes which features are most used, how users navigate the app, crash reports, and general usage trends. We use these insights to debug issues (for instance, to investigate a crash report from your app version), optimize user interface and experience, and decide what new features to build. In many cases, analytics data is aggregated and doesn't directly identify you; if any personal data is involved, we ensure any third-party analytics providers only use it on our behalf and under instructions (see "Sharing" below). For example, we might use Google Analytics on our website to understand page visit patterns, or use in-app analytics to see how long users spend on the profile section versus the match section. These help us make data-driven decisions to improve functionality and content.

- **Advertising and Marketing (if applicable):** Currently, MusLinc's primary business is to provide a great dating service, and our monetization may come from optional subscriptions or premium features. We do not currently serve third-party banner ads or sell your data to outside parties for marketing. However, in the event we introduce advertising or partnerships in the future, we may use certain data (like cookies or device identifiers) to deliver relevant advertisements within the app or to promote MusLinc on other platforms. For instance, we might work with advertising partners like Google or Facebook to show ads for MusLinc to people with similar interests. This could involve sharing hashed or identifier information to match user profiles on those platforms for "custom audience" advertising. If we ever engage in this type of activity, we will update our policies and obtain any necessary consents in compliance with laws. Additionally, we may occasionally run contests, surveys or refer-a-friend programs; information you provide in those contexts will be used strictly for those purposes (e.g., to administer the contest or apply referral rewards) and as otherwise described at the time of collection.

- **Legal Compliance and Protection of Rights:** We may process your personal data when necessary to comply with legal obligations to which we are subject. This includes retaining certain records to satisfy tax, accounting or regulatory requirements, responding to valid legal requests (such as court orders or subpoenas) or cooperating with law enforcement investigations as required by law. We will carefully review any request to ensure it has proper legal basis before disclosing data. We also process data as needed to enforce our Terms & Conditions and other agreements, or to establish, exercise or defend legal claims. For example, if there is a dispute or legal claim involving a user, we may preserve relevant data and share it with our legal advisors or authorities as appropriate. Similarly, we may use personal information to investigate or address fraud, security breaches, or other potentially harmful or illegal activities on the platform. Our aim is to protect the rights, property, and safety of our users, MusLinc, and the public. This may include using data to block abusive users, alert potential victims (if we believe someone's safety is at risk), or provide anonymized evidence in reports to law enforcement (for instance, if required to report certain content involving minors). We will notify users of any legally compelled disclosure of their information, if we are allowed to do so.

Legal Bases for Processing (UK & EU users): If you are in the UK or European Economic Area, we rely on the following legal grounds under UK GDPR/EU GDPR to process your information:

- **Contractual Necessity:** Much of our data processing is to fulfill our contract with you – i.e., to provide the Services you have requested. When you agree to our Terms & Conditions and use MusLinc, a contract is formed, and we need to process your data (like profile info, matches, messages, etc.) to perform that contract by providing the app's functionality. For example, we process your basic account data and communications under this basis.

- **Legitimate Interests:** We process certain data as necessary for our (or others') legitimate interests, except where overridden by your data protection rights. Our legitimate interests include maintaining a safe and secure platform, preventing fraud and unauthorized use, improving our Services, and, where permitted, marketing our Services to interested users. We carefully consider and balance any potential impact on your rights before relying on legitimate interests. For example, it is in our legitimate interests to process data to detect fake accounts or to keep basic logs for security, as this benefits our community's safety without unduly infringing on user privacy. Similarly, using analytics to improve user experience is a legitimate interest. If we send you promotional offers about MusLinc and you are an existing customer, we may do so under legitimate interests, but you can always opt out of such marketing.

- **Consent:** Where required by law, we rely on your consent. For instance, we ask for your consent to process special category data (like your religious beliefs) that you add to your profile. By providing that information voluntarily, you consent to our processing of it for the purpose of sharing on your profile and related matchmaking. You may withdraw that consent at any time by removing such information from your profile (which will prevent us from processing it further). We also obtain your consent to use certain cookies or similar technologies for analytics/advertising on our website, as described in our Cookie Policy, when such consent is required. If we ever introduce third-party advertising that involves sharing your personal data, we would seek your consent as needed. Additionally, if you opt in to receive newsletters or direct marketing communications from us (such as by ticking a box or selecting preferences in the app), we process your email and possibly usage data under consent for that specific purpose. You have the right to withdraw your consent at any time (for example, by unsubscribing from emails or changing your app settings), and we will stop the relevant processing.

- **Legal Obligation:** In some cases, we must process certain data to comply with a legal obligation. For example, if a law requires us to retain transaction records for a certain period (for tax or financial regulations), we process those under legal obligation. If we receive a lawful court order to provide information, processing that data for compliance is based on legal

obligation. Likewise, our duties under consumer protection laws or privacy laws themselves (such as honouring your data rights requests) may form a legal basis.

- **Vital Interests:** This is less likely to apply, but if processing is necessary to protect someone's life or prevent serious harm, we might rely on vital interests. For instance, in rare emergency situations where there is an imminent threat to someone's safety and we need to contact authorities and share data, that could fall under this basis.

We will normally clarify at the point of collection which basis applies if it's not obvious, and we remain committed to transparency about our practices.

3. Optional Features and Modes

MusLinc includes some optional features designed to enhance your experience and safety. These features involve additional uses of your data, and by choosing to use them, you agree to the related data processing:

- **Photo/ID Verification Badge:** As mentioned earlier, we require a selfie verification during sign-up to ensure that every profile is authentic. Completing this step successfully may result in a "Verified" badge on your profile, indicating to other users that MusLinc has confirmed your profile photos are really you. On occasion, or for certain features, we may offer additional verification options, such as verifying your government ID or confirming details like your occupation or education. These are voluntary. If you choose to verify, say, your ID, we (or our Verification Provider AWS) will process that document and related data only to confirm elements like your name or age. Upon successful verification, we might display a tick mark or label on your profile (e.g., "ID verified") to build trust. Any such program will come with instructions at the time of use. By undertaking a verification, you agree to let us (and our authorized agent) process the data in that document for verification purposes. We do not store the actual ID image long-term after verification; we keep a record that verification was completed and the result. **Disclaimer:** A verification badge means that a specific check was performed and passed (for example, that your selfie matched your profile photos, or your ID confirms you are 18+). It does not guarantee that a user is completely "safe" or that they have no bad intentions. Always exercise the same caution in interacting with verified users as you would with unverified users. AWS (aws.amazon.com) is a tool to reduce catfishing and misrepresentation, but it is not a background check or endorsement of character.
- **Location-Based Matching:** If you grant us location access, MusLinc can use your location to improve your match results by showing you people near your area or in specified locations you are interested in. In your profile settings, you may be able to set a "preferred location" (for example, if you are open to matches in a particular city or region beyond your current GPS location). We use your device's location and any location preference you set to filter and sort potential matches. For example, you might see matches within a certain radius of your city. We may also display approximate distance or location information on profiles (e.g., "London, 5 miles away"), though you can disable showing your distance if you prefer. **Privacy of location:** We do not reveal your precise address to other users. We typically show city or general area. You can choose in settings whether to hide your distance. Location data also helps us with trust and safety: we may compare the location of your device against the location listed in your profile and other signals to detect inconsistencies or possible impersonation. If a profile is found to be falsifying location or if we detect use of GPS spoofing, we might reject or suspend the profile to maintain authenticity. You are free to turn off location sharing at any time via your device/app permissions; doing so will limit location-based features but you can still manually set a location on your profile if allowed. Our use of location is continuous while you use the app (to update and deliver relevant results), but we typically do not track your background location when the app is completely closed, unless you opt into features that need it. If we ever introduce a feature like showing your real-time proximity to others (perhaps for an event), it will be opt-in.
- **Paid Subscriptions and Features:** MusLinc may offer premium subscription plans (e.g., a monthly membership with added perks) or one-time paid features (like sending a gift, boost, or other enhancements). If you opt to subscribe or purchase, additional terms apply (see our Terms & Conditions). From a data perspective, opting into premium features might involve additional data usage – for example, if a premium feature allows you to be seen by more users, we will adjust our algorithms to promote your profile (meaning more users' apps will load your profile data). If a feature allows you to see extra information (say, seeing who liked you), we will use your data to compile those insights. Rest assured, we handle all personal data in the context of premium features with the same care as standard features. If any premium feature were to require processing your data in a new way not covered by this Privacy Policy, we will provide specific notice when you opt in.
- **Events or Social Features:** Occasionally, MusLinc might host optional events (virtual or in-person) or introduce community features like forums or group chats. Participation in these is voluntary. If you join an event or group, information you share there (like messages in a public forum or your attendance at an event) may be visible to other participants or even publicly if it's an open forum. We will clarify the audience of any such feature. We will use your data (like profile and contact info) to manage event registrations and attendance. For example, if it's an in-person meetup, we might have a guest list of names. We may also gather feedback or photos from events to promote community engagement (with your consent where needed). Any new feature of this sort will come with updated guidelines on data use.

4. Cookies and Similar Technologies

MusLinc uses cookies and similar tracking technologies on our website and within our app to ensure our Services function correctly and to enhance your experience. A “cookie” is a small text file that websites send to your device to store information about you, such as your preferences or login status. In the context of mobile apps, similar identifiers (like mobile advertising IDs or in-app tokens) serve a comparable purpose. Here’s how we use these technologies:

- **Types of Cookies/Trackers We Use:**

- **Essential Cookies:** These are necessary for our website or app to operate. For example, they help with logging you in and keeping you logged in, or remembering your session so you don’t constantly have to re-enter information. They also help maintain security by, for instance, keeping track of your session ID to prevent hijacking. Without these, certain basic functions would not work. Note: Because these are strictly necessary, they are generally used without requiring your consent (except via your browser settings). They do not gather information for marketing, only for service functionality.
- **Preferences/Functional Cookies:** These cookies remember choices you’ve made to personalize your experience. For instance, if our website has a language selector or if you’ve dismissed a certain pop-up, a cookie might remember that so we can load the site in your chosen language or avoid showing you something you’ve already seen. They make the site/app tailored to you. For example, we might use a cookie to save your cookie consent preferences.
- **Analytics Cookies:** We use these to collect information about how users interact with MusLinc. They tell us things like which pages are visited, how long users stay, how they navigate through the app, and any issues encountered (like error messages). This data is aggregated and helps us improve the Service’s performance and design. For example, analytics cookies can show if a new feature is being used by many users or not, informing our decisions. We may use third-party analytics tools like Google Analytics which set their own cookies; however, these tools are only allowed to use the data to provide services to us (not for their own advertising or other purposes) and we configure them to anonymize data where feasible (for instance, Google Analytics can anonymize IP addresses).
- **Advertising & Marketing Cookies:** As of now, MusLinc does not display third-party ads on our platform. However, if we run marketing campaigns for MusLinc on other websites, we might use cookies or pixels to measure their success. For example, a Facebook Pixel on our sign-up page could tell us how many people who saw our ad actually registered. If in the future we introduce on-platform advertising or partnerships, we might allow certain advertising cookies that help tailor ads to your interests or limit how many times you see an ad. These could collect data about your browsing habits on our site/app and potentially combine with info from other sites. If that happens, we will update our Cookie Policy and obtain appropriate consent. We will also give you the ability to opt out of targeted advertising cookies. We commit that we will not share personally identifying information with third-party advertisers without your consent. Advertising cookies, when used, are typically persistent until they expire or you clear them (meaning they remember you on repeat visits). They help in “interest-based advertising,” ensuring any ads you see are more relevant and not just random.
- **Social Media Cookies:** If our site has sharing plugins or you connect your account via a social network, those third-party platforms may set cookies. For example, a “Share on Facebook” button might allow Facebook to set a cookie to see if you are logged in and to facilitate the sharing. These cookies might track your activity across websites where they are present (for instance, if you are logged into Facebook, Facebook might know you visited our site). We do not control these cookies, so we encourage you to check the respective platform’s privacy policies. We include this category so you’re aware, but these cookies would usually require your consent (via the third party’s arrangement or via our site’s cookie banner if applicable).
- **Mobile App Identifiers:** In our mobile app, we don’t use “cookies” per se, but we use SDKs (software development kits) and device identifiers. For example, we might use Firebase or similar analytics SDK in the app to gather usage stats. These act similarly to cookies by assigning a unique random ID to your app installation to track how you use the app. If we eventually support third-party login or integration, those services’ SDKs might collect data similarly. We treat these identifiers with the same level of transparency and control as browser cookies. You can typically reset your mobile device’s advertising identifier or limit ad tracking in your device settings if advertising becomes relevant.
- **Consent and Control:** When you first visit our website, you will be presented with a cookie notice or banner if non-essential cookies are in use. We will ask for your consent to set analytics or marketing cookies. You can choose which categories of cookies you accept (except the strictly necessary ones, which are always on). If you accept some and later change your mind, you will have the option to adjust your preferences. We provide a cookie settings link on our site (often in the footer or in your profile settings when logged in) for you to review or change your preferences at any time. In the mobile app, you may have controls in your account settings to toggle certain analytics or personalized advertising preferences. Additionally, regardless of our site’s tools, you can manage cookies through your browser settings. All major browsers allow you to see what cookies are stored, delete them, and set rules to reject cookies from all or specific sites. For instance, you can usually find these options under “Privacy” or “Security” settings in your browser. Please note that blocking all cookies (especially essential ones) might cause portions of our Service to not work properly – for example, you might not be able to log in or your preferences might not be saved. If you clear cookies, that also means if you had

opted out of certain cookies via our banner, that opt-out cookie might be deleted and you'd need to set it again.

- **Similar Technologies:** As mentioned, we may use technologies like pixels, web beacons, and SDKs which function similarly to cookies. A pixel or web beacon is a tiny graphic or script embedded in a webpage or email that usually isn't visible to the user. It can track if you've opened an email or visited a page. For example, we might include a pixel in our newsletter emails to know if recipients opened the email, helping us gauge interest in our communications. In the app, an SDK might collect info like the app version, platform, and user actions to send to our analytics server. For simplicity, we refer to all these as "cookies" or "tracking technologies" in our policies. Rest assured, in all cases, these technologies are used in line with the purposes described and with respect to applicable legal requirements.
- **Do Not Track and Global Privacy Control:** "Do Not Track" (DNT) is a setting available in some browsers that sends a signal to websites indicating a user's preference not to be tracked across sites. At this time, there is no industry standard for how to respond to DNT signals, and accordingly, our systems may not recognize or react to DNT headers. However, users have the more granular control described above (consent choices, browser settings). There is also an emerging signal called Global Privacy Control (GPC) which is intended as a way for users to signal their privacy preferences (specifically to opt out of sale/sharing of data under laws like CCPA). If we detect a GPC signal from your browser and you are known to be in a jurisdiction like California, we will treat it as a valid opt-out of any third-party marketing/advertising cookies on our site (as if you had declined those in our cookie banner). We will also interpret it as an opt-out of "sale" of personal info, which, as we explain below, we do not currently do anyway.

For more information on how we use cookies, you can refer to our full Cookie Policy (if provided as a separate document or section). By using MusLinc, you agree that cookies and similar technologies may be placed on your device, as described, unless you disable them. We strive to make our use of these tools transparent and to give you control. If you have any questions about our Cookie Policy or need assistance with adjusting your preferences, please contact us.

5. How We Share Your Information

We treat your personal information with care and do not sell it. However, we do need to share information with certain trusted third parties and other users in order to run our business and provide the Services. The categories of recipients of personal data include:

- **Other MusLinc Users:** MusLinc is a social/dating platform, so information you include in your profile will be visible to other registered users of the Service. This includes profile photos, first name, age, location (as specified by you or approximate based on city/region), and other details you choose to share on your profile such as biography, interests, and religious or cultural background (if you provided them). Keep in mind that any information or content you post on your profile or share through the app could potentially be seen, copied, or re-shared by others, so only include information you are comfortable being public in the MusLinc community. We design the app to discourage abuse – for instance, we may blur or watermark images to prevent unauthorized copying – but we cannot control how someone you connect with might use the information you make available. For example, if you share your phone number or social media handle with another user in a chat, that is at your own risk (we recommend waiting until you trust someone before sharing contact info off platform). We prohibit users from displaying others' personal contact details publicly, but private exchange is your choice. Additionally, if you send content (like a message or photo) to another user, they will obviously see it, and they may save it or show it to someone else; use discretion. If a match is made (both users like each other) we facilitate the exchange of messages and other features between you and that other user – by necessity, that involves sharing your chosen name, profile info, and the contents of your chats with the person you're talking to (as that is the nature of communication). We do not ever display your precise location or your last name to other users through the standard profile interface. Other users might infer information about you based on what you share (for instance, your photo might reveal your ethnicity or if you wear religious attire; your manner of speech in chats could indicate things about you). That is within your control via what you share.
- **Public Content:** At this time, MusLinc does not have a public feed or forum visible to non-users. Should we introduce any feature where content can be seen by a broader audience (for example, a success story or testimonial you submit for our blog, or a public event posting), we will clarify that at the point of submission. We might, for instance, publish anonymized statistics or success stories (with your consent). But by default, only logged-in users can see profile details, and only those you match with can see your detailed profile or chat with you, etc., according to our design.
- **Service Providers ("Processors"):** We employ trusted third-party companies and individuals to help us operate, provide, and improve our Services. These third parties perform functions under our direction and on our behalf pursuant to contracts that ensure your data is protected. They are not allowed to use your data for their own unrelated purposes. Examples of service providers we use include:
 - **Hosting and Infrastructure:** Companies that provide cloud hosting, data center storage, and server operations for MusLinc (for example, Cloud Service Provider hosting our databases and servers in secure facilities). They store data such as profile information, messages, and photos on our behalf. These providers are rigorously vetted for security and privacy practices, and we remain in control of the data.

- **Analytics Services:** Third parties that help us understand usage of our platform (like Analytics Partner). They may receive device identifiers, usage data, and other analytics information (possibly via cookies or SDKs as described above). This data is generally aggregated and not personally identifiable, but even if some identifiers are included, the analytics provider is contractually bound to use the information only to deliver insights to us and not for other purposes.

- **Payment Processors:** If you make purchases, we rely on external payment gateways (e.g., Stripe for card processing, or if you purchase via Apple's App Store or Google Play, then Apple or Google processes the payment). These entities will receive personal information necessary to process the transaction, such as your name, billing address, and payment details. We share the minimum required information and do not see or handle your full credit card number ourselves. Payment processors are data controllers for your payment info in their own right, but they can also be seen as our service providers processing the fact you made a purchase. They typically provide us with a transaction ID and status.

- **Email and Communication Tools:** We may use third-party platforms (like Email Service Provider) to send out emails, such as verification emails, newsletters (if subscribed), or support communications. These platforms will handle your email address and the content of the emails under our instructions. Similarly, push notification services (like Apple Push Notification service for iOS or Firebase Cloud Messaging for Android) deliver app notifications to your device; they get minimal info (just what is needed to route the message).

- **Customer Support Software:** If you contact us for support via chat or email, we might use a customer support management tool (like Support Ticket System) which will process your contact info and the correspondence to help us track and respond to your inquiry.

- **Verification and Fraud Prevention:** As discussed, we use specialized vendors like AWS (Identity Verification service for selfie/ID checks). For example, AWS (aws.amazon.com) will receive your selfie and perhaps ID document and process it to verify your identity. They generate a result and share it with us. They might temporarily hold the biometric or document data during the process, but as per our agreement and the law, they delete or anonymize it after use. Another example: a service that checks phone numbers to prevent fake accounts will get your number for that one-time check and confirm validity. All such partners are bound by confidentiality and strong data protection terms.

- **Content Moderation Tools:** We may use automated moderation software or external moderators (bound by contract) to help review content (profiles, messages, images) reported or flagged for policy violations. For instance, an image recognition service might screen profile photos for nudity or graphic content so we can keep it off the platform. These tools may process user content, but they do not use it for anything other than flagging policy issues to us.

- **Advertising and Marketing Partners:** If we engage in marketing, we may share limited data with advertising platforms to reach potential new users or re-engage existing ones. For example, we might upload a list of user email addresses (in hashed form) to a platform like Facebook or Google to create "custom audiences" for MusLinc ads, meaning show our ad to people on those platforms who are our users or similar to them. Or we might use an ad network to run ads on other apps, which could involve sending a device ID and some context (like "this device installed MusLinc, show them our promotion"). These activities are only done if permitted by law (with consent if required). We do not provide your personal details to advertisers for them to use for their own unrelated marketing. We also do not currently have third-party ads in our app that would involve tracking by external advertisers. If that changes, we will update our policies and obtain consents.

In all cases with service providers, we share only the information necessary for them to perform their function. We also require that they implement appropriate technical and organizational measures to protect your data, in compliance with UK GDPR and similar laws. A list of our key sub-processors can be provided on request (and may be listed on our website), so you can see who we work with. Examples might include cloud providers like AWS or Azure, analytics like Google Analytics, messaging services like Twilio (if we send SMS), etc.

- **Business Partners and Affiliates:** Currently, MusLinc is a standalone service provided by MusLinc Ltd. If in the future we become part of a group of companies or form partnerships, we may share information within that corporate family or partnership as needed to operate the service. For example, if we establish a branch in the EU to serve European users, we may transfer UK user data to our EU subsidiary for localized support and vice versa. All such intra-group transfers will comply with applicable laws and this policy (and if outside the UK, appropriate safeguards). We may also share information with co-branding partners or promotional partners with your consent. For instance, if we co-host an event with a community organization and you sign up for the event, we might share your name with the co-host purely for event administration. Or if we have a feature where you can choose to share certain data with a partner (like participating in a research study or a matchmaking service), we will only do so with your knowledge and agreement. We do not broadly share user data with third parties for their own independent use without user permission.

- **Legal and Compliance Sharing:** We may disclose your personal information when we believe in good faith that such disclosure is necessary to:

- **Comply with a legal obligation:** This could be responding to lawful requests by public authorities (e.g., a court order, subpoena, government demand). We will ensure the request has appropriate jurisdiction and scope. If the request comes from outside your country, we may refuse or challenge it unless it's via proper international channels (like a mutual legal assistance treaty).
- **Meet national security or law enforcement requirements:** If required by law, we might have to provide information for law enforcement or national security. UK GDPR (and equivalent laws) allow exceptions in certain cases. We will try to be transparent with users if allowed – for example, if law enforcement requests data about you, we may notify you unless we are legally prohibited or it's an emergency.
- **Protect and defend the rights or property of MusLinc:** For example, disclosing information to our legal counsel or debt collectors if we're enforcing a payment or investigating fraud affecting us.
- **Prevent or investigate possible wrongdoing in connection with the Services:** If we suspect a user has committed fraud or a cybercrime targeting our platform or users, we might share data with cybersecurity consultants or other platforms to mitigate it.
- **Protect the personal safety of users or the public:** If someone is at risk of harm (like violence or self-harm) and we have data that could prevent it, we might share information with authorities or those who can help, as appropriate.
- **Protect against legal liability:** If we face legal action or potential claims, we may disclose data as evidence or to demonstrate compliance (for instance, providing records that show we acted lawfully).

We always aim to handle such requests with care and strictly limit what is disclosed. We also may require a warrant or court order for content, as per law. Non-content information (like basic subscriber info) may be given under different standards, but we still ensure it's lawful. We also publish (in reports or on request) the number and type of government requests we receive, if any, as part of our transparency commitment.

- **Business Transfers:** In the event MusLinc undergoes a business transaction such as a merger, acquisition by another company, reorganization, sale of all or part of its assets, or in the unlikely event of bankruptcy or receivership, user information (including personal data) may be among the assets transferred to or acquired by a third party. The new owner or combined entity would continue to honour the commitments we've made in this Privacy Policy (or put in place a comparable privacy protection for you). We would ensure any such transfer is permissible under applicable law – for example, if required, we'd give you notice or seek your consent when your data is about to be transferred and become subject to a new privacy policy. Similarly, if we undergo any internal restructuring, data may be shared within our affiliates (as mentioned above) but still protected under this policy's terms.
- **Aggregate or De-Identified Information:** We may share information that has been aggregated (combined with other data so it no longer identifies you personally) or de-identified (stripped of personal identifiers) with third parties for various purposes. For example, we might share statistics like "X% of our users are in London" or "the average age of users is Y" for research or marketing purposes. This data cannot be linked back to individual users. We may also share general usage trends with partners or the public in blog posts or reports (e.g., highlighting how many matches were made in a year). These kinds of disclosures do not impact your privacy and are typically not limited, as they contain no personal data.

We want to emphasize that we do not sell your personal information to third parties for profit. "Selling" under some laws (like the CCPA) is defined broadly to include sharing for certain advertising purposes. As of the date of this policy, MusLinc does not share personal data with third parties for them to market their own products to you. If that ever changes, we will update this policy and provide an opt-out.

If we ever have to share your information in a manner not covered above, we will do so only with your consent. For instance, if a television show or academic study wanted to contact some of our users for a feature and we thought you might be interested, we would first come to you and ask if you want to participate – we wouldn't just hand out your info.

A more detailed list of third-party sub-processors and partners can be found on our website/at the end of this policy if you're interested in the specific vendors and entities that may handle your data.

6. International Data Transfers

MusLinc is based in the United Kingdom, but our users may be from various countries, and our service providers might also be located internationally. This means that your personal information could be transferred and stored in countries outside of your own, including countries outside the UK or the European Economic Area (EEA). For example, if you are in the UK, some of your data might be processed on servers in the United States or the European Union, or if you're in the EU, your data might be accessed by our UK operations.

UK & EU Users: The UK and EU have strict rules for transferring personal data to countries that are not deemed to have "adequate" data protection laws. Whenever we transfer personal data out of the UK (or EEA), we will ensure a similar

degree of protection is afforded to it as under UK/EU law. We typically use one or more of the following safeguards:

- **Adequacy Decisions:** The UK (and EU) have approved certain countries as providing adequate protection for personal data. For example, data can flow freely from the UK to EEA countries (and vice versa) because the UK has deemed the EU adequate, and currently the EU has deemed the UK adequate post-Brexit. If you're an EU user, note that the EU has an "adequacy decision" for the UK, so transfers between the EU and UK are allowed. Beyond that, if we ever transfer data to, say, Canada or Japan (countries with adequacy decisions), those are covered by adequacy as well.
- **Standard Contractual Clauses (SCCs)/International Data Transfer Agreement (IDTA):** For transfers to countries without an adequacy finding (such as the United States, if data goes there), we use the standard contractual clauses (SCCs) approved by the European Commission and/or the UK's International Data Transfer Agreement/Addendum, as applicable. These are legal contracts that bind the recipient to protect the data according to EU/UK privacy standards. For instance, many of our service providers in the U.S. have signed SCCs with us to cover UK/EU user data they might process. These clauses contain obligations like: the data importer must handle data securely, must respect data subject rights, and if there's any conflict with local law that would prevent compliance, they must inform us and possibly suspend transfers. We've also reviewed, where relevant, whether additional technical measures (such as encryption) are needed on top of SCCs for certain transfers, in line with the Schrems II ruling.
- **Binding Corporate Rules (BCRs):** This would apply if we were part of a corporate group with approved internal rules for data transfers. At this time, we don't have BCRs, but if in future MusLinc grows and adopts BCRs for internal transfers, we will mention it.
- **Explicit Consent or Other Exceptions:** In rare cases, we might rely on your explicit consent to transfer data (for example, if you're participating in a one-time specific activity abroad). We could also rely on necessary transfer for contract performance (like if you're traveling and using the app in a different country, we have to send your data to that country to provide the service). But our general approach is to rely on the structured safeguards like SCCs for routine transfers.

Regardless of where your data is processed, we apply the same protections described in this Privacy Policy. We also contractually require that our non-UK/EEA processors handle data in compliance with applicable privacy standards. For instance, our U.S. cloud provider is certified under frameworks like ISO 27001 and has committed in the SCCs to maintain EU-level privacy.

For Users Outside the UK/EEA: By using MusLinc, you understand that your data may be transferred to the UK and other jurisdictions as needed. If you're in a country like the US or Canada, your data will likely be stored in the UK and/or cloud servers possibly in the EU or US. We ensure compliance with local laws for users in those areas too. For example, if you're a user in California, any transfers of your data internationally are done in accordance with CCPA's requirements (though CCPA doesn't restrict transfers specifically, it does require safeguarding personal info generally). If you're in a country like India or Australia, we still maintain strict confidentiality and security regardless of transfer.

External Websites and Services: Keep in mind, when you click on links in our app that take you to third-party websites (like an article link, or an Instagram profile, etc.), those are outside our control. If you go to an external site, any data you provide to that site is subject to their policies. Similarly, if you use an external payment service (like Apple or Google in-app payments), those transactions might involve transfers according to those companies' arrangements (for example, Apple may process worldwide transactions in the US). We encourage you to review the privacy practices of any third-party services you access through MusLinc.

If you would like more information about our international data transfer practices or to obtain a copy of the relevant transfer mechanism (like SCCs), you can contact us at [Contact Email](#). We may provide some details in a summarized form for confidentiality reasons (for instance, our SCCs might contain proprietary clauses or security annexes we can describe rather than share outright), but we'll do our best to address your concerns.

7. Data Retention

We retain your personal data only for as long as necessary to fulfill the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements. How long we keep information depends on the type of information and the purposes for which we use it. Below are our general retention practices:

- **Account Data and Profile Information:** We will keep your profile information, account credentials, and content you've provided for as long as you maintain an active account with us. If you decide to delete your account (or if we terminate it due to inactivity or violation), we will initiate deletion of your personal data from our live systems. In general, when you delete your account, we will deactivate it immediately and remove or anonymize your personal data within timeframe, e.g., 30 days. However, we may retain certain information for longer if needed for legitimate business or legal purposes (see below). For example, when an account is deleted, your profile is no longer visible to others and is disassociated from any content (messages will show a "deleted user"), and your personal info will be purged from our main user database after the retention period.

- **Chats and Communications:** Messages you send to others are stored as part of the conversation. Even if you delete your account, the messages you sent may still be retained in the recipient's inbox (they will appear under a generic user or "deleted member" label, but content might remain to preserve the integrity of their chat history). We generally do not purge one user's messages from another user's inbox unless specifically requested by a remaining user or if required by law. However, if both users in a conversation have deleted their accounts, the chat content will be deleted. If you want your messages deleted, you would need to request that under your privacy rights (but note, rights like erasure can be limited where they infringe on others' rights to keep their data – e.g., the other user's chat record). For internal retention: even after deletion, we might keep backup copies of chat data for a certain period (e.g., in encrypted backups or logs) which are then overwritten per our backup retention schedule, unless flagged for a specific reason.

- **Media (Photos, etc.):** Profile photos and other media you upload are stored to provide the service. If you delete a particular photo or video from your profile, it will no longer be visible in the app shortly after. We then delete the file from our storage within a reasonable time (it might persist in cached or CDN servers for a short period). If you delete your account, all your photos and media are queued for deletion as well. We maintain secure backups, so a copy of a deleted item might remain in backup storage for a limited time until those backups cycle out – during that period, it's not accessible through the app.

- **Sensitive Data:** Any special category data (like religious views) you provided in your profile is treated like other profile info – removed when you remove it or when your account is deleted. Biometric verification data (like the unique identifier from a facial recognition) is not stored by us at all ; it's handled by "AWS" and they delete it promptly after verification. We do keep your verification status (e.g., that you are verified) indefinitely until account deletion, as that's needed to know whom to show as verified.

- **Usage Logs:** We maintain logs of certain activities (like sign-in times, IP addresses, device info, errors) to troubleshoot and secure the service. These logs are usually retained for a shorter period, say 90 days, unless required for security analysis. For instance, IP logs may be kept to investigate fraud or to comply with any law enforcement request directives. After that, they may be aggregated or deleted.

- **Legal & Safety Retention:** If we have suspended or banned your account due to violations, we may retain certain information indefinitely to prevent you from circumventing the rules (for example, your email, phone, and device ID may be kept on a blacklist to enforce a permanent ban). Similarly, information relating to reports of bad behaviour, harassment complaints, etc., may be kept as long as needed to protect us or others from repeat offenders. We also retain records if needed to establish, exercise, or defend legal claims. For example, if we remove content due to a copyright takedown notice, we might keep records of that takedown. If we receive a subpoena or hold notice related to your data, we will preserve relevant info until the issue is resolved. In a scenario like detecting a serious scam, we might keep data on it to cooperate with law enforcement or to analyse and prevent it happening again.

- **Financial Records:** We keep purchase and subscription records for at least as long as required by tax and accounting laws. In the UK, for instance, transaction records might be kept for 6 years for tax audit purposes. However, these records would contain minimal personal info (e.g., amount, date, order reference, maybe your user ID or email as customer identifier) and not your full card details. Similarly, if a refund was issued, we'd keep that record.

- **Backups:** Our system likely does routine backups. Backup data is encrypted and safely stored. It is typically retained for a limited retention period (maybe 30-90 days rolling) purely for disaster recovery. If data is deleted from live systems, it will remain in backups until those backups expire and are overwritten. We treat backups with high security and do not restore data from them except for rare restoration needs.

- **Anonymized Data:** In some cases, rather than outright deletion, we may anonymize your personal data so that it can no longer be associated with you. For instance, after a certain period, we might convert some data to statistical information. If we have anonymized data, we may retain and use it indefinitely, as it no longer identifies you and is not personal data.

Once our retention periods are over, we will securely erase or anonymize your personal information. We base our retention schedule on criteria like the volume, nature, and sensitivity of the data; the potential risk of harm from unauthorized use or disclosure if we keep it; the purposes of processing and whether those can be achieved by other means; and applicable legal requirements.

For example, as a guideline (subject to change and specific exceptions as above):

- If your account is inactive (no logins) for 12 months, we may send you a notice and then delete your account data if you do not respond. We'd remove the account similarly to a user-initiated deletion.

- After account deletion, personal data is purged from active databases typically within 30 days, and residual info in backups is gone within 90 days.

- Communications with customer support might be retained for 2 years in case of follow-ups, then deleted.

- Logs and analytics data are usually rotated or aggregated after several months.

These are illustrative. We have a detailed internal data retention policy that ensures we don't keep personal data longer than necessary. If you have a specific question about how long a certain type of data is kept, you can contact us for more precise info.

8. Your Rights and Choices

You have several rights in relation to your personal data under applicable data protection laws. MusLinc is committed to honouring these rights and providing you with appropriate control and transparency. Below, we outline your key rights and how you can exercise them:

- **Right to Be Informed:** You have the right to be informed about the collection and use of your personal data. This Privacy Policy is part of fulfilling that right by explaining what data we collect, why, and how we handle it. We aim to be transparent and will notify you of significant changes to how we use your information (for example, if we start processing it for a new purpose). In-app, we might also present contextual notices (like just-in-time notifications asking for permission to use location, explaining what for). If you have any questions about our data practices beyond what's in this policy, you can always ask us.
- **Right of Access:** You can request confirmation of whether we are processing your personal data, and if so, ask for a copy of the personal data we hold about you. This is commonly known as a "Data Subject Access Request." You are entitled to receive your data in a concise, transparent, intelligible format, along with details such as the purposes of processing, the categories of data, who we share it with, and the storage period. We will provide this information free of charge, usually within one month of your request (unless the request is complex or numerous, in which case we may extend by up to two further months, but we'll inform you if so). How to exercise: You can contact us at Contact Email to request your data. For your and others' security, we may need to verify your identity (for example, by confirming control of your account or asking for certain information) before releasing data. The output will likely include things like your profile info, message history, etc., that constitute personal data. Note that certain data may not be included if it does not qualify as personal data (e.g. anonymized analytics) or if it involves others' personal data (we might redact third-party info from your copy). We might also provide it via a secure means, like a downloadable file.
- **Right to Rectification:** If any personal information we hold about you is inaccurate or incomplete, you have the right to have it corrected. The easiest way to rectify your data is often by logging into your account and editing your profile or settings (you can update things like your profile details, photos, preferences, etc., at any time). For any information you cannot self-edit (perhaps your email or something locked), you can contact us and we will correct it upon verification. We strive to keep our records up to date, so we appreciate any updates you provide. If we've shared incorrect data with others, we will inform them of the rectification where possible.
- **Right to Erasure (Right to be Forgotten):** You have the right to request deletion of your personal data in certain circumstances. This is not an absolute right, but we will honour it when applicable. You can delete your account at any time through the app's settings – this is the most direct way to exercise erasure, as it triggers our deletion process described above. Additionally, you can specifically request that we erase certain information (for example, if you posted something and want it removed, though typically you can remove content yourself). We will delete data on request if:
 - The data is no longer necessary for the purposes we collected it for.
 - You initially consented to processing and later withdraw consent (and we have no other legal grounds to keep processing).
 - You have objected to processing (see below) and we have no overriding legitimate grounds to continue.
 - We processed your data unlawfully.
 - There is a legal obligation to erase the data.
 - The data was collected from a child (which we don't do, but if hypothetically an underage user's data was collected).

If your request for erasure is valid, we will erase the data and also take steps to inform any third-party processors or partners who had the data to erase it as well (for instance, if we had shared data with a service provider, we'll convey the deletion request to them, except where it's impossible or requires disproportionate effort). We will confirm to you when we've deleted the data. Note: In some cases, we may refuse or defer deletion. For instance, if you request deletion of data that we are required by law to keep (e.g., transactional records), or if deletion would undermine other users' free expression rights (e.g., you posted in a forum and deletion of your account would also erase others' contributions that rely on it – not usually the case in a one-to-one chat scenario). If we cannot fulfil part of an erasure request, we'll explain why (unless legally prevented). Also, if you simply deactivate or uninstall the app, that's not the same as deletion – please use the delete option or contact us.

- **Right to Restrict Processing:** In certain situations, you have the right to ask us to restrict (pause) the processing of your personal data. This means we would store your data but not actively use it until the restriction is lifted. You can request

restriction if:

- You contest the accuracy of the data – for the period while we verify its accuracy, processing can be restricted.
- The processing is unlawful and you oppose erasure, requesting restriction instead (for example, you want us to keep the data but not use it, perhaps for a legal claim you have).
- We no longer need the data, but you need it for the establishment, exercise, or defence of legal claims.
- You have objected to processing (see next bullet) and we are considering whether our legitimate grounds override yours.

When processing is restricted, we will not use or share the data except for storing it, or to establish/exercise/defend legal claims, or protect someone's rights, or other limited reasons allowed by law. We will inform you before lifting a restriction. If your profile is under restriction, for example, your profile might be hidden from others in that time.

- **Right to Object:** You have the right to object to certain types of processing of your personal data on grounds relating to your particular situation. The main instances for this are:
 - **Direct Marketing:** You can object at any time to processing of your personal data for direct marketing purposes. If you object, we will stop using your data for marketing immediately. This includes profiling related to direct marketing. Practically, this means if you say no to marketing, we'll stop sending you newsletters or promotional offers. Note that even if you opt out of marketing, we may still send you transactional or service messages (like account notices).
 - **Legitimate Interests Processing:** If we are processing your data based on our legitimate interests (or those of a third party), you can object if you believe it impacts your rights and freedoms. We will then re-evaluate our reasons for processing. We will stop processing unless we have compelling legitimate grounds that override your interests, rights, and freedoms, or unless continuing to process is necessary for us to establish, exercise, or defend legal claims. For example, you might object to some analytics processing – if it's not crucial, we may agree and stop processing your data in that way.
 - **Research or Statistical Purposes:** If we were processing data for research or statistics, you could object on grounds relating to your situation, unless it's necessary for a task in the public interest.

To object, you can contact us with your request specifying what processing you object to. For marketing, it's simpler: just use the "unsubscribe" link in emails or toggle off marketing in your app settings. For other objections, we may ask for details about your particular situation so we can properly weigh the factors.

- **Right to Data Portability:** You have the right, in certain scenarios, to receive the personal data you have provided to us in a structured, commonly used, machine-readable format, and have the right to transmit that data to another service provider. This applies when the processing is based on your consent or a contract and is carried out by automated means. For example, you might want to port your profile info and photos to another app. We will provide the data in a format like JSON or CSV that is widely accepted, which should include data like your profile details, your messages (where feasible), etc. You can request we send it directly to another provider if technically possible, otherwise we give it to you to handle. The portability right doesn't cover data that is about you but that you didn't provide (like profiles others wrote about you, or internal notes), and it doesn't automatically include derived data (like analytics inference). However, we aim to include as much of your core data as possible. If you require this, reach out and we'll guide you.
- **Rights Related to Automated Decision Making and Profiling:** You have rights to not be subject to decisions based solely on automated processing, including profiling, which have legal or similarly significant effects on you. MusLinc does not engage in fully automated decision-making with legal or significant impact without human involvement. For instance, our matchmaking suggestions are automated, but you are not bound by them, and they do not have a legal effect on you. If we ever were to implement something like automated rejection or acceptance of profiles (which we currently do not; any account bans involve human review), you would have the right to contest that decision and request human intervention. Rest assured, currently most important decisions (like banning for misconduct) involve human moderation. You do have the right to ask for information about our algorithmic processes (which we've described somewhat in this policy – e.g., we use algorithms for matching). If you believe you've been adversely affected by an automated process, let us know and we'll review it.
- **Right to Withdraw Consent:** In cases where we rely on your consent to process data, you have the right to withdraw that consent at any time. For example, you may have consented to us using your precise location or to processing your special category data (like religious info) – you can withdraw by changing settings (turn off location, remove the religious info from your profile) or contacting us. Withdrawal of consent will not affect the lawfulness of processing that happened before the withdrawal, but it means we will stop the specific processing going forward. If you withdraw consent for a particular feature (say, biometric verification usage), we'll inform you if that means we can no longer provide that feature to you.

• **California Privacy Rights (CCPA/CPRA):** If you are a California resident, you have specific rights under the California Consumer Privacy Act (as amended by the CPRA) in addition to those above. These include:

• **Right to Know:** You can request that we disclose the categories and specific pieces of personal information we have collected about you, the categories of sources, the business or commercial purpose for collecting (or selling/sharing, if applicable) the information, and the categories of third parties with whom we share it. Much of this is covered in this Privacy Policy. You also have the right to know if we have sold or shared your personal information or disclosed it for a business purpose (and if so, what categories to whom). Note: MusLinc does not sell personal information for monetary consideration. We also do not “share” personal information as defined by CPRA (meaning share for cross-context behavioural advertising), because we currently don’t share data with third-party ad networks in a way that would be considered a sale or sharing. If that ever changes, we will provide a “Do Not Sell or Share My Personal Information” link to allow you to opt-out. As of now, we treat any California Do Not Sell signals accordingly (we simply don’t sell/share anyway). You can exercise the right to know by contacting us, and we will provide the required information (largely mirroring what’s in this policy but specific to you).

• **Right to Delete:** Largely similar to the above-described right to erasure. California residents can request deletion of their personal info we have collected and retained, subject to certain exceptions. Upon a verified deletion request, we will delete and instruct our service providers to delete your info, unless an exception applies (e.g., we need to keep it for legal reasons or certain internal uses).

• **Right to Correct:** Similar to rectification, California residents have the right to request correction of inaccurate personal information we hold.

• **Right to Opt-Out of Sale or Sharing:** As noted, while we don’t engage in those practices, California law gives you the right to opt-out. We honour global opt-out signals like GPC if detected. If in future we started sharing data for advertising, we would implement a clear opt-out mechanism.

• **Right to Limit Use of Sensitive Personal Information:** Under CPRA, if we collect “sensitive personal information” (SPI) – like precise geo, racial or ethnic origin, religious beliefs, etc. – and use it for purposes beyond what’s considered necessary to provide the services, California residents can direct us to limit its use and disclosure to allowed purposes. In our case, we collect some sensitive info (e.g., religion, possibly biometric via verification) but only for the core service or security (which is generally considered within the allowed uses). We don’t use sensitive info to infer characteristics or for targeted advertising. Thus, we don’t require a “Limit SPI” link because we’re not using it in a secondary way. If you have concerns, you can contact us.

• **Right of Non-Discrimination:** We will not discriminate against you for exercising any of your CCPA rights. This means we won’t deny you the service, charge you a different price, or provide a lesser experience just because you exercised privacy rights. If you are a paying user and you delete your data or opt-out of some sharing such that we can no longer provide a certain feature, we’ll inform you, but we won’t unfairly treat you differently for making a privacy choice. We might, at most, be unable to offer a certain perk if it inherently requires some data use (for example, if an optional feature relies on location and you opt-out of location, you just won’t use that feature, but that’s not discrimination – it’s a consequence of your choice which we’ll communicate).

California users (or their authorized agent) can submit requests through our contact email or any webform we provide. We will need to verify identity for these requests (e.g., verifying account ownership). For disclosure or deletion requests, verification might involve confirming details we have on file. Agents must have permission; if you use an agent, we require proof of authorization and maybe direct confirmation from you.

• **UK and EU Users – Complaint Rights:** If you have concerns about our data handling, we’d like you to contact us so we can resolve it. However, you also have the right to lodge a complaint with a supervisory authority. In the UK, that is the Information Commissioner’s Office (ICO). You can find their contact details and complaint process on the ICO website. For EU users, you can contact the data protection authority in your country of residence. For example, in Ireland it’s the Data Protection Commission, in France the CNIL, in Germany the local state DPAs, etc. You typically would go to the one in the country where you live or work or where the issue happened. They will advise or investigate as needed. We hope it never gets to that, and we are committed to privacy compliance.

• **Communication Preferences:** For non-essential emails (newsletters, etc.), you can use the unsubscribe link in the email footer or adjust preferences in the app (often under Notifications settings). For push notifications, your phone’s OS settings allow you to turn those off if you no longer want them.

• **Account Settings:** We encourage you to review your in-app account settings regularly. There you may find options to do things like download your data (if we implement a self-serve data export), manage blocking of other users, etc. We plan to continually enhance user controls.

To exercise any of your rights or if you need assistance, you can reach out to our privacy team at privacy@muslinc.com. We will respond to your request as soon as possible, generally within one month. If we need more time (up to a total of

three months for complex requests), we will inform you of the delay and the reason. Please note, for security, we must ensure it's you (or your authorized agent) making the request, so we might ask for certain information to verify identity, especially for sensitive requests like access or deletion. This is to protect your data from unauthorized access.

9. Security Measures

We employ appropriate technical and organizational security measures to protect your personal data against unauthorized access, alteration, disclosure, or destruction. MusLinc takes security seriously, and while no platform is 100% immune to threats, we follow industry best practices to safeguard your information. These measures include:

- **Encryption:** All network communication to and from our app and website is encrypted using HTTPS/TLS. This means that personal data (like login credentials, messages) is transmitted securely and cannot easily be intercepted. Sensitive data in our databases (for example, passwords) is hashed or encrypted at rest. Passwords are stored using secure hashing algorithms (we never store them in plain text). Certain sensitive fields may be additionally encrypted in our database (such as any identification documents, if we ever store any temporarily). Our servers or cloud storage also employ encryption at rest for stored data, adding an extra layer of protection against data theft.
- **Access Controls:** Access to personal data within our organization is restricted on a need-to-know basis. Only authorized personnel (such as specific staff in customer support, moderation, or engineering roles who need access to perform their job) can access user data, and even then, it's limited to what they need. For example, our support team may have tools to look up your profile or see chat reports if you raise an issue, but they won't unnecessarily browse messages without cause. We maintain strict access logs and use multi-factor authentication for administrative access to our systems. Our staff and any contractors are bound by confidentiality obligations.
- **Security Testing & Audits:** We regularly test and evaluate our systems to identify vulnerabilities. This includes routine software updates (keeping servers and libraries patched), vulnerability scanning, and periodic penetration testing by security experts. We also operate an internal bug bounty or responsible disclosure program to encourage ethical reporting of any security flaws. Our infrastructure is monitored for suspicious activities, and we have intrusion detection systems in place. We also audit our service providers for their security measures; we choose reputed providers (for example, data centers with ISO 27001 or SOC 2 compliance) and ensure they adhere to equivalent security standards.
- **Anonymization & Pseudonymization:** Where feasible, we pseudonymize data in our internal processes – e.g., separating direct identifiers from activity data. For analytics, we often use aggregated data. This means that even if some analytics data were compromised, it wouldn't directly identify individuals. Special category data (if any) might be segregated to further limit access. We also avoid using real user data in testing environments – we use dummy data for development and testing where possible.
- **Physical Security:** If any personal data is stored on physical servers, those servers are in secure facilities with controls like surveillance, access badges, and security personnel. However, being a modern app, much of our storage is likely cloud-based. Our cloud providers also implement strict physical security at their data centres.
- **Training:** We train our employees about privacy and security best practices. Everyone at MusLinc is aware of data protection principles and is required to follow company policies on data handling. We limit the use of portable media or local storage of personal data; primarily, everything stays in our controlled environment.
- **Backups and Recovery:** We maintain backups (with encryption) to ensure data isn't lost accidentally and we can recover from any technical issues quickly. However, backups are protected and only accessed for restoration or disaster recovery tests.
- **Account Security Tips:** While we do our part, user behaviour is crucial too. We encourage you to use a strong, unique password for MusLinc and to keep your login credentials confidential. We will never ask you for your password via email or chat. Be cautious of phishing attempts; always make sure you're logging in through our official app or website. If you suspect any unauthorized access to your account, change your password immediately and notify us.

It's important to note that despite all these efforts, no method of transmission over the internet or method of electronic storage is completely secure. Therefore, we cannot guarantee absolute security. In the unlikely event of a data breach that is likely to result in a high risk to your rights and freedoms (for instance, a breach exposing sensitive or financial info), we will inform you and the relevant authorities as required by law (within the timelines set by regulations like UK GDPR). We have a breach response plan in place to quickly mitigate and notify as appropriate.

If you have reason to believe that your data is no longer secure (for example, if you feel your account has been compromised), please contact us immediately so we can assist.

10. Third-Party Links and Services

Our Services may contain links to third-party websites or integrate with third-party services (such as social media login or map services). For example, user profiles might have an option to link to an Instagram account, or we might integrate

Google Maps for location selection. If you click on a link to any external website or service, or if you interact with third-party content through MusLinc, this Privacy Policy does not apply to that third party. Those sites and services have their own privacy policies, and we do not accept any responsibility or liability for their policies or how they handle your data. We encourage you to read the privacy statements of each third-party service you visit or use.

Specific examples:

- **Social Media and Login Integrations:** If you register or log in via a social platform like Google or Facebook, the authentication is handled by that platform under its own privacy terms. They may collect info such as the fact that you used their login on MusLinc. We only receive the data we need (like your email and name) from them. Similarly, if you share content from MusLinc to a social network, that action is governed by the social network's policy.
- **External Profiles or Websites:** If a user shares a link to an external profile or website in their chat or profile and you click it, we're not responsible for what that site does with any data. Be careful and only click links from people you trust.
- **Advertisements:** Right now, we don't have third-party ads, but if we did, those ads might link out to advertiser sites. Clicking an ad would take you away from our app and to their domain.
- **Third-Party Content:** Sometimes, we might embed third-party content (like a YouTube video in a help article). Viewing that embedded content might allow the third party (YouTube in this case) to collect data (like via cookies or logging). They should inform you via their own cookie notices, etc.

In summary, once you leave MusLinc or interact with a non-MusLinc entity, their rules apply, not ours. However, if a third-party integration within our app is misbehaving or causing privacy concerns, please let us know, as we want to ensure everything in our environment aligns with our standards.

11. Children's Privacy

MusLinc is not intended for anyone under the age of 18, and we do not knowingly collect personal information from children (under 18). We explicitly prohibit minors from creating accounts. Our registration process asks for your date of birth to ensure you meet the age requirement, and we implement verification steps to prevent underage usage (such as requiring selfie verification which can sometimes flag obviously underage appearances, though it's not foolproof). If we discover that a user is under 18, we will take immediate action to terminate the account and delete all associated data. For example, if a 16-year-old signs up falsifying their age and we later find out (say, through a report or during verification) that they are underage, we will ban the account and wipe their info.

If you are a parent or guardian and you become aware that your minor child has created an account or otherwise provided us with personal data, please contact us immediately. We will promptly remove the information and terminate the account in accordance with applicable laws. We rely on users to be truthful about their age (and it is in violation of our Terms to lie about it). We take this seriously because the platform involves interactions that are only appropriate for adults.

We also note that in some jurisdictions, the age of majority may be older than 18 (for example, in some places it's 19 or 21 for certain services). Our policy is 18 globally, but if local law requires a higher age for a user to lawfully use a service like ours, then we will observe that.

12. Updates to this Privacy Policy

We may update or revise this Privacy Policy from time to time to reflect changes in our practices, technologies, legal requirements, or other factors. If we make material changes (for example, changing the types of data we collect, or how we use it, or if we start sharing data with new types of third parties), we will provide you with prominent notice. This may include: posting a notice within the MusLinc app, updating the effective date at the top of the policy, and/or emailing you or otherwise messaging you about the change.

We encourage you to review this policy periodically to stay informed about how we protect your information. If you continue to use MusLinc after any changes to the Privacy Policy take effect, you will be considered to have agreed to the updated policy. However, if any change requires your consent (under applicable law), we will obtain that consent.

For minor or clarifying updates that don't materially affect your rights, we might simply update the policy and indicate the date of revision on the top without a pop-up or email, but the latest version will always be accessible via the app or our website.

If you do not agree with the changes to the Privacy Policy, you should stop using our services and may delete your account. We'll always aim to give you the choice wherever feasible.

13. Contact Us

If you have any questions, concerns, or requests regarding this Privacy Policy or how MusLinc handles your personal data, please do not hesitate to reach out to us:

- Email: privacy@muslinc.com – This is our dedicated channel for privacy inquiries.
- Postal Mail: Data Protection Officer, MusLinc Ltd, Tottenham Court Road Suite 6621a, Fitzrovia, London, United Kingdom, W1T 2EW

We will address your inquiry as promptly as possible, typically within 30 days. If you are contacting us to exercise a data subject right, please clearly state which right you wish to exercise and provide relevant details to help us verify your identity and locate your data (e.g., the email associated with your account).

If you have a concern about our handling of your data, we genuinely want to resolve it in a fair and transparent manner. Reaching out to us directly is usually the quickest way to get an answer or solution.

Thank you for reading our Privacy Policy. Your trust is important to us, and we are committed to safeguarding your personal information while providing you with a great platform to connect with others.