Privacy Policy

SafeSpace

Mobile peer mental health support application

Last updated: March 19, 2026

Application processing mental health data — high sensitivity level

This policy applies to an application processing sensitive personal information of a psychological and emotional nature. Enhanced protection measures apply at all times, in accordance with Quebec Law 25 and privacy best practices.

SafeSpace does not replace professional mental health services

SafeSpace is a peer support community tool.

Call 911 for any medical or immediate safety emergency.

Quebec Suicide Crisis Line: 1-866-277-3553 (24/7)

Crisis Montreal: 514-934-4433

Tel-jeunes (under 21): 1-800-263-2266

Canada Suicide Prevention Line: 1-833-456-4566 (24/7)

1. Purpose and Scope

This Privacy Policy describes how SafeSpace (9528-5896 Québec Inc.) (“SafeSpace”, “we”, “us”) collects, uses, communicates, retains, and protects personal information in connection with the operation of the SafeSpace mobile application, in accordance with:

- Quebec’s Act to modernize legislative provisions as regards the protection of personal information (Law 25);
- The Personal Information Protection and Electronic Documents Act (PIPEDA);
- Guidelines issued by the Commission d’accès à l’information du Québec (CAI).

SafeSpace is a Canadian mobile application incorporated in Quebec, dedicated to creating small peer support groups focused on mental health and overall well-being. It is available to Canadian residents aged 16 and over. Due to the highly sensitive nature of the information processed, we apply the highest privacy protection standards.

Privacy by Design

SafeSpace integrates privacy protection into the design of its features from the outset. Each new feature undergoes a Privacy Impact Assessment before deployment.

2. Person Responsible for Personal Information

In accordance with Law 25, SafeSpace designates a person responsible for personal information:

Name: Mathis Grenier

Position: President

Privacy Email: privacy@appsafespace.com

General Email: admin@appsafespace.com

This person is responsible for:

- Ensuring compliance with privacy laws and this policy;
- Handling access, correction, and deletion requests;
- Managing privacy incidents and maintaining the required incident register;
- Supervising Privacy Impact Assessments;
- Ensuring internal privacy awareness and training.

Response Time

SafeSpace will respond to privacy rights requests within a maximum of 30 calendar days.

3. Minimum Age, Consent and Protection of Minors

SafeSpace is available only to individuals aged 16 and older. No person under the age of 16 may register on the platform.

3.1 Age Verification

During registration:

- Mandatory confirmation of date of birth;
- Automatic blocking of registrations under age 16;
- Immediate account deletion if a false age declaration is discovered.

3.2 Additional Measures for Ages 16–17

Due to the sensitive nature of the data processed, users aged 16 and 17 are subject to the following additional measures:

- Explicit age confirmation during registration;
- Recommendation to inform a parent or responsible adult;
- Periodic reminders encouraging consultation with a professional in case of distress.

3.3 Intervention in Case of Imminent Risk

If there is a serious or imminent risk to a user's safety, whether minor or adult, SafeSpace may:

- Contact emergency services;
- Transmit only the minimum necessary information to authorities;

- Temporarily suspend or restrict access to the account concerned.

3.4 Withdrawal of Consent for Minors

A minor (16 or 17) may withdraw consent at any time via:

- The “Delete my account” feature in the application;
- A written request to privacy@appsafespace.com.

All data will be deleted within 15 business days, except security logs required by law.

4. Collection of Personal Information

SafeSpace follows the data minimization principle: only information strictly necessary for each purpose is collected.

We collect information:

- During account creation and management;
- When using application features;
- When contacting support;
- Automatically for technical operation.

4.1 Registration Data

During registration, we collect:

- Email address: required (for authentication and essential communications);
- Username: pseudonyms allowed and encouraged;
- Password: encrypted;
- Date of birth: required for age verification;
- Profile photo: optional.

4.2 Content Shared Voluntarily

Users may voluntarily share sensitive information. These data points are never mandatory and you retain control over their content and deletion:

- Posts and comments in SafeSpaces;
- Private messages via the Reach Out feature;
- Personal journal entries: visible only to you;
- Emotion tracking data via the emotion wheel;
- Personal descriptions and wellness goals.

Control of your sensitive data

Users may delete any content at any time. Deletion is completed within a reasonable timeframe and no later than 30 days, in accordance with our retention schedule (Section 9).

4.3 Automatically Collected Data

Minimal technical data is collected automatically for technical operation and security:

- Device type and OS version;
- Approximate IP address (security purposes only);
- Crash logs: anonymized;

- Aggregated usage statistics.

SafeSpace does not perform advertising profiling or commercial targeting.

5. Sensitive Personal Information and Granular Consent

SafeSpace processes sensitive personal information that may reveal:

- Emotional state and psychological well-being;
- Mental health challenges, vulnerabilities, or personal crises;
- Trauma or difficult life experiences;
- Gender identity or sexual orientation.

5.1 Consent Levels

SafeSpace uses granular consent levels. You may accept or refuse each category independently:

- **Level 1 — Essential operation (required):** data minimal required for account creation and security.
- **Level 2 — Community participation (optional):** posts, comments, private messages. You may participate in read-only mode.
- **Level 3 — Personal wellness tools (optional):** journal, emotion wheel, goals. These remain private.
- **Level 4 — Service improvement analytics (optional):** aggregated statistics and email options.

Users may modify consent preferences at any time in Privacy Settings.

5.2 Protection of Sensitive Data

Sensitive data protections include:

- Encryption at rest and in transit (AES-256 and TLS 1.3);
- Restricted access to authorized personnel;
- Separation between identity data and sensitive data;
- Pseudonymization for internal analytics;
- No commercial or advertising use.

6. Purposes and Legal Bases for Processing

Data is processed for:

- **Providing the service:** account management, SafeSpaces, messaging. Legal basis: contract execution.
- **Safety and moderation:** prevention of harassment, risk intervention. Legal basis: legitimate interest.
- **Service improvement:** anonymized analytics. Legal basis: consent.
- **Legal obligations:** incident registers, cooperation with authorities. Legal basis: legal obligation.

No incompatible secondary use is performed.

7. Technology Infrastructure, Security and Privacy by Design

7.1 Security Measures

SafeSpace uses Convex as its primary backend infrastructure. Security measures include:

- TLS encryption in transit;
- AES-256 encryption at rest;
- Secure authentication;
- Role-based access control (RBAC);
- Separate development/test/production environments;
- Encrypted backups;
- Access logs retained for 90 days.

7.2 Risk Assessments and Audits

SafeSpace maintains a proactive security program:

- Privacy Impact Assessments before any new processing;
- Annual security reviews;
- Vulnerability testing;
- Access permission reviews.

7.3 Data Transfers Outside Canada

If data is transferred outside Canada:

- Privacy Impact Assessments are conducted;
- Equivalent contractual protections are implemented.

7.4 Privacy Incident Management

SafeSpace maintains a formal incident procedure:

- An incident register retained for 5 years;
- Notification to authorities and users when required;
- Post-incident review procedures.

Reporting an incident

If you notice unauthorized use of your information, report it to privacy@appsafespace.com.

8. Communication and Sharing of Personal Information

SafeSpace does not sell personal information. Information may be shared only:

- **With user consent:** for any sharing not provided for in this policy.
- **With essential service providers:** hosting, security, infrastructure providers subject to strict confidentiality.
- **When required by law:** by court order or authority.
- **To prevent imminent danger:** to emergency services.
- **During corporate transactions:** mergers or acquisitions.

8.1 Internal Access and Facilitators

Access is limited to authorized personnel:

- **Moderators:** access to reported content only.
- **Facilitators:** access to their assigned SafeSpaces only, no access to journal or private messages.
- **Technical staff:** anonymized logs for maintenance.
- **Management:** for administrative and legal obligations.

9. Retention and Destruction of Information

SafeSpace applies defined retention periods for each category of data:

Data Category	Retention Period	Destruction Method
Registration data (email, username, DOB)	Account life + 12 months	Secure erasure
Profile data (gender, photo)	Account life	Immediate erasure on request
Posts, comments in SafeSpaces	Account life	Erasure within 30 days
Private messages (Reach Out)	24 months after last message	Secure erasure
Personal journal	Account life	Immediate erasure on request
Emotion tracking data	12 months (rolling)	Anonymization or erasure
Technical logs (IP, crash data)	90 days	Automatic purge
Security logs (incidents)	5 years (legal obligation)	Secure archiving
Minor data	Account life + 6 months	Priority erasure

Deletion delay after account closure: Personal data is erased from active servers within 30 days. Some content already received by other users may remain in their history; they can delete it on their end.

Information is destroyed securely according to category:

- Digital data: secure erasure following recognized best practices;
- Backups: purged during the next rotation cycle (max 90 additional days);
- Legal logs: encrypted archiving with strict access control.

10. User Rights

In accordance with Law 25, you have the following rights with guaranteed response times:

Right	Description	Response Delay
Access	Obtain a copy of your info held by SafeSpace	30 days
Rectification	Correct inaccurate or incomplete information	30 days
Deletion	Erase your data, subject to legal obligations	30 days
Withdrawal	Stop non-essential processing, without retroactive effect	Immediate
Portability	Receive your data in a structured, commonly used format (e.g., JSON or CSV)	30 days
Objection	Object to certain treatments (e.g., aggregated analysis)	30 days

10.1 How to exercise your rights

To exercise your rights, you have two channels:

- **In the application:** Settings → Privacy → Manage my data.
- **By email:** privacy@appsafespace.com specifying your username and the right being exercised.

10.2 Recourse to CAI

If you believe your rights have not been respected, you may file a complaint with the **Commission d'accès à l'information du Québec (CAI)**: www.cai.gouv.qc.ca

11. Account Deletion

Users may delete their account at any time via Settings → Account → Delete my account. Before definitive deletion, you can:

- Download a copy of your data (export);
- Individually delete your posts, comments, and private messages;
- Temporarily deactivate your account without deleting data.

12. Pseudonymization and Anonymous Participation

SafeSpace encourages pseudonymous participation:

- The use of a pseudonym is authorized and encouraged;
- Email addresses are never visible to other users;
- Analytics data is anonymized or pseudonymized before processing;
- No link is established between your pseudonym and real identity in reports.

13. Limitation of Liability

SafeSpace is a peer support community tool. It is not a professional mental health service, crisis line, or emergency service. SafeSpace is not responsible for:

- Advice, opinions, or information shared by users;
- Personal decisions made following interactions on the platform;
- Interactions or meetings organized between users outside the application.

14. Modifications of the Policy

Users will be notified of significant changes via the application. Significant modifications involving sensitive data will require new explicit consent.

15. Language and Interpretation

This Privacy Policy was originally drafted in French. An English version is provided for convenience and accessibility. In the event of any discrepancy, inconsistency, or difference in interpretation between the French version and the English version, the French version shall prevail and constitute the official legal version.

16. Contact

Privacy Officer

privacy@appsafespace.com

Administration

admin@appsafespace.com

Post Address

6595 St-Urbain Street, Montreal QC H2S 3G6, Canada

17. Glossary

- **Personal Information:** Any information concerning a natural person that allows them to be identified directly or indirectly.
- **Sensitive Personal Information:** Information whose disclosure is likely to cause serious harm to the person, notably health or psychological info.
- **Consent:** Free, informed, and specific manifestation of will by which a person accepts the processing of their data.
- **Privacy Impact Assessment (PIA):** Analysis mandatory before any new treatment of sensitive data.
- **Anonymization:** Irreversible treatment making identification impossible.
- **Privacy Incident:** Unauthorized access, use, or destruction of personal information.

18. Effective Date

This Privacy Policy has been in effect since March 19, 2026, and replaces any prior version.