

Privacy Policy

FLINTCOMPANY Inc. (ABNORMAL CHAT)

FLINTCOMPANY Inc. (hereinafter referred to as the "Company") has established and publicly discloses this Privacy Policy in accordance with Article 30 of the Personal Information Protection Act of the Republic of Korea to protect the personal information of its users and to promptly and smoothly handle related grievances.

This Policy applies to the AI chat service "ABNORMAL CHAT" (hereinafter referred to as the "Service") operated by the Company.

Article 1. Categories and Methods of Personal Information Collection

1. Categories of Information Collected

A. Required Information at Registration

- Email address
- Password (stored in encrypted form)
- Nickname

B. Optional Information at Registration

- Age (age range)
- Region of residence

C. Information Automatically Collected During Service Use

- Conversation content with AI characters
- Memory data analyzed and generated by AI (conversation summaries, emotional patterns, relationship records, etc.)
- Relationship temperature and moment note data
- Service usage records (access date/time, IP address, device information, OS version)
- Push notification tokens (Expo Push Token)
- Payment records (in-app purchase receipt information — payment amount, product name, transaction ID)

D. Payment Information

- In-app purchase (IAP) receipt data (transaction information issued by Apple/Google)

* The Company does not directly collect financial information such as credit card numbers or bank account numbers. All payments are processed through the Apple App Store and Google Play.

2. Methods of Collection

- Directly entered by users during registration and onboarding
- Automatically generated and collected during service use
- Payment information received through in-app purchase platforms (Apple/Google)

Article 2. Purpose of Collection and Use of Personal Information

The Company uses collected personal information for the following purposes:

Purpose	Details
Member Management	Registration, identity verification, prevention of unauthorized use, grievance handling
Service Provision	Providing AI character chat service, operating memory system for conversation context retention, delivering personalized content
Payment Processing	In-app purchase processing, subscription status management, Soul (credit) top-up and deduction
Notification Service	Sending push notifications (character messages, service announcements, etc.)
Service Improvement	Statistical analysis of service usage, AI conversation quality improvement, new service development

Article 3. Provision of Personal Information to Third Parties

The Company processes personal information only within the scope specified in Article 2 and does not, in principle, process beyond the original scope or provide it to third parties without the prior consent of the user.

However, exceptions are made in the following cases:

- When the user has given prior consent to third-party provision
- When required by special provisions of law or to comply with legal obligations
- When it is clearly necessary for the urgent protection of life, body, or property of the user or a third party, and the user or their legal representative is unable to express consent or cannot be reached

Article 4. Outsourcing of Personal Information Processing

The Company outsources personal information processing as follows for smooth service provision:

Service Provider	Outsourced Tasks	Retention Period
Supabase Inc.	Database hosting and authentication services	Until end of outsourcing contract or member withdrawal
Render Services, Inc.	Backend server hosting	Until end of outsourcing contract

xAI Corp. (Grok API)	AI conversation response generation	Immediately upon completion of API call processing
Anthropic PBC (Claude API)	AI conversation response generation (paid tier)	Immediately upon completion of API call processing
Expo (Expo Go, LLC)	Push notification delivery	Immediately upon delivery completion
Apple Inc. / Google LLC	In-app purchase processing	Per each company's policies

The Company stipulates necessary provisions to ensure the safe management of personal information in outsourcing contracts.

Article 5. Retention and Use Period of Personal Information

The Company processes and retains personal information within the retention and use period required by law or agreed upon with the user at the time of collection.

1. Member Information

Retained until membership withdrawal and destroyed immediately upon withdrawal. However, if retention is required by applicable laws, the information is retained for the legally required period.

2. AI Conversation and Memory Data

Destroyed upon membership withdrawal or upon the user's request for deletion.

3. Retention Periods Required by Law

Records	Period	Legal Basis
Records on contracts or withdrawal of offers	5 years	Act on Consumer Protection in Electronic Commerce
Records on payment and supply of goods/services	5 years	Act on Consumer Protection in Electronic Commerce
Records on consumer complaints or dispute resolution	3 years	Act on Consumer Protection in Electronic Commerce
Records on labeling and advertising	6 months	Act on Consumer Protection in Electronic Commerce
Service usage records, access logs, IP addresses	3 months	Protection of Communications Secrets Act

Article 6. Procedures and Methods of Personal Information Destruction

The Company destroys personal information without delay when it is no longer necessary due to the expiration of the retention period, achievement of the purpose of processing, or other reasons.

1. Destruction Procedure

Unnecessary personal information is destroyed within 5 days from the date it is deemed no longer necessary.

2. Destruction Methods

- Electronic files: Permanently deleted using methods that prevent recovery and reproduction
- Paper documents: Shredded or incinerated

Article 7. Rights and Obligations of Users and Legal Representatives

Users (or legal representatives in the case of users under 14 years of age) may exercise the following rights regarding personal information protection at any time:

- Right to request access to personal information
- Right to request correction of errors
- Right to request deletion
- Right to request suspension of processing

These rights may be exercised through 'My Page > Edit Profile' within the Service or by contacting our customer support email (linkeelive@gmail.com). The Company will take action without delay.

If a user requests correction or deletion of personal information due to errors, the Company will not use or provide such personal information until the correction or deletion is completed.

Article 8. Special Provisions Regarding AI Conversation Data

Due to the nature of the ABNORMAL CHAT service, the following data is generated and processed during conversations with AI characters:

1. Conversation Content

Messages sent by users to AI characters and AI responses are stored for maintaining conversation context and improving service quality.

2. AI Memory System

Information extracted by AI from conversations with users (such as names, interests, and emotional states) is stored and utilized to provide a natural conversational experience. Users may request deletion of AI memory at any time.

3. Transmission to Third-Party AI Models

Conversation content is transmitted to the APIs of external AI service providers (xAI, Anthropic) for AI response generation. Transmitted data is processed according to each service provider's policies, and the Company requires data protection through contracts with these providers.

4. Precautions

Users are advised not to enter sensitive personal information such as national identification numbers or financial information in conversations with AI characters. Users are responsible for information entered during conversations.

Article 9. Measures to Ensure the Security of Personal Information

The Company takes the following measures to ensure the security of personal information:

- Encrypted storage and management of passwords
- Restriction and management of access to personal information
- Encryption of network segments through SSL/TLS
- Database access control (Row Level Security policies applied)
- Retention of access records for personal information processing systems
- Security measures against hacking and other threats

Article 10. Operation of Cookies and Automatic Collection Devices

ABNORMAL CHAT is a mobile application and does not use web cookies.

However, device identifiers, access logs, and usage records may be automatically collected during service use and are utilized for service operation and quality improvement.

Article 11. Personal Information Protection Officer

The Company has designated the following Personal Information Protection Officer to oversee personal information processing and handle complaints and remedies related to users' personal information:

Category	Details
Name	Wooyeol Jeong
Position	CEO (Representative Director)
Email	makesflint@gmail.com
Phone	+82-10-4685-8226
Customer Support Email	linkeelive@gmail.com

Users may contact the Personal Information Protection Officer regarding any inquiries, complaints, or remedies related to personal information protection arising from the use of the Service. The Company will respond and process such inquiries without delay.

Article 12. Remedies for Rights Infringement

Users may apply for dispute resolution or consultation with the following organizations for relief from personal information infringement:

Organization	Contact	Website
Personal Information Dispute Mediation Committee	1833-6972	www.kopico.go.kr
Personal Information Infringement Report Center (KISA)	118	privacy.kisa.or.kr
Supreme Prosecutors' Office Cyber Investigation Division	1301	www.spo.go.kr
National Police Agency Cyber Bureau	182	ecrm.police.go.kr

Article 13. Personal Information of Children Under 14

The Company does not accept membership registration from children under the age of 14 and does not collect personal information from children under 14.

Article 14. Changes to this Privacy Policy

This Privacy Policy may be amended due to changes in laws, policies, or security technologies. Any changes will be announced through in-app notices or push notifications at least 7 days prior to the effective date.

Supplementary Provisions

This Privacy Policy is effective as of March 19, 2026.

FLINTCOMPANY Inc.
CEO Wooyeol Jeong