SNK INTERACTIVE_ Personal Information Handling Policy

June 11, 2025

Privacy Policy

Article 1 (Purpose):

This policy is established to disclose the collection, sharing, retention, disposal, protection, and operation of personal information related to services provided by SNK Interactive Co., Ltd. (”the Company”), including internet services via wired/wireless and on/offline game services. "Services" refer to all accessible services provided by the Company, regardless of the type of wired or wireless device.

Article 2 (Collected Personal Information and Methods):

The Company collects the following personal information for membership registration, customer service, member interaction, and service provision:

1. Email address, password, and nickname at the time of registration.
2. Additional personal information such as gender, age, profile photo, and greeting after registration.
    - Services without separate consent procedures for items 1 and 2 do not collect the corresponding information.

Additionally, the following information may be collected:

- Device information, service connection details (e.g., application data), automatically generated data, IP address, recent login time, location information, phone number, device-specific identifiers (UDID/IMEI), usage history, and records of inappropriate use.
- Automatically during service use.
- Voluntarily provided by members during service usage or registration.
- Payment details such as card or mobile phone usage history during paid service transactions.

Article 3 (Purpose of Collection and Use of Personal Information):

- To identify users by combining device type and unique identifiers (e.g., device ID

or IMEI) with phone numbers.

- To facilitate member interactions through shared profile information (e.g., status messages, nicknames, photos).
- For identity verification, grievance handling, communication of notices, and prevention of improper service usage.
- For developing new services, marketing, and advertising.
- To provide tailored services, analyze usage statistics, display targeted advertisements, and assess service efficiency.
- To manage inquiries and fulfill customer service needs related to contracts, payments, refunds, and disputes for paid services.

Article 4 (Sharing and Disclosure of Personal Information):
The Company does not use or disclose personal information beyond the purposes outlined in Article 3 without prior consent from members, except in the following cases:

- When consent is provided by the member.
- When necessary to fulfill service-related contracts.
- For billing purposes associated with service provision.
- When required by law or investigative purposes under legal procedures.
- When special provisions are stipulated in laws such as the Real Name Financial Transactions Act, Consumer Protection Act, etc.

Article 5 (Retention and Usage Period of Personal Information):
Personal information is retained until the user withdraws their membership or the purpose of collection is fulfilled. Afterward, it is promptly deleted. However, the following information may be retained for specific periods according to company policies:

- **Upon Membership Withdrawal:**
    - Reason: Prevention of improper use (Internal Policy)
    - Retention Period: 1 year
- **Records Related to Identity Verification:**
    - Reason: Based on the Act on Promotion of Information and

Communications Network Utilization and Protection

  - Retention Period: 6 months

- **Service Access Records:**
  - Reason: Protection of Communications Secrets Act
  - Retention Period: 3 months
- **Consumer Complaints or Dispute Resolution Records:**
  - Reason: Consumer Protection Act in E-Commerce
  - Retention Period: 3 years
- **Records Related to Contracts or Withdrawals:**
  - Reason: Commercial Act, Consumer Protection Act in E-Commerce
  - Retention Period: 5 years
- **Records of Payments and Supply of Goods:**
  - Reason: Commercial Act, Consumer Protection Act in E-Commerce
  - Retention Period: 5 years

Article 6 (Procedure and Methods for Destroying Personal Information):

- Personal information provided by members for registration and service usage is transferred to a separate database (or separate document storage for paper-based records) after the purpose is fulfilled. It is stored for a designated period according to internal policies and relevant laws (see retention and usage periods) before being destroyed.
- Personal information is not used or shared for purposes other than those required by law.
- Personal information printed on paper is destroyed by shredding or incineration.
- Electronic files storing personal information are deleted using technical methods that make recovery impossible.
- If a member deletes the app without withdrawing their membership, their personal information may still be retained by the service provider. In this case, members need to separately request withdrawal from the service provider.

Article 7 (Installation, Operation, and Rejection of Automatic Collection Devices):

- Members have the right to refuse consent to the collection of personal information under the Personal Information Protection Act. However, refusal to consent will result in the inability to use the service.
- Device identifiers (e.g., device ID or IMEI) are automatically collected when the member runs the service to create account information.
- Location information may be collected via the location service embedded in the member's device to display the distance between members within the service.

Article 8 (Technical and Managerial Protection Measures for Personal Information):
The company takes the following measures to ensure the safety of personal information and prevent loss, theft, leakage, tampering, or damage:

1. Members' personal information is protected by passwords, and IDs and passwords are encrypted, stored, and managed securely. Only the user knows this information, and ID change functionality is not provided.
2. Efforts are made to protect against personal information leaks or damage caused by hacking or computer viruses.
3. Firewalls and other protective measures are used to safeguard personal information and data. Every possible technical security device is implemented.
4. Personal information handling is limited to designated employees who are given unique passwords for access. Employees are regularly educated to ensure compliance with the privacy policy.

Article 9 (Moving to Third-Party Sites):

- The company may provide links to third-party websites or materials. The company has no control over external sites or resources and is not associated with their privacy policies or terms. Members must verify the policies of these sites to avoid any disadvantages or damages. Responsibility for issues arising lies solely with the user.

Article 10 (Contact for Personal Information Management):
Members can report any privacy-related complaints that occur during the use of the company's services to the personal information management officer or the designated department. The company will promptly and adequately respond to such reports.

Personal Information Management Officer:

- **Name:** Representative Jeon Se-hwan
- **Email:** [Not provided in the text]

※ If you need to report or consult about other privacy violations, please contact the following organizations.

Personal Information Breach Reporting and Consultation Contacts:

- **Personal Information Breach Reporting Center:** http://privacy.kisa.or.kr/ / Phone: 118
- **Information Protection Mark Certification Committee:** www.eprivacy.or.kr / Phone: 02-580-0533~4
- **Supreme Prosecutors' Office, Cyber Crime Investigation Division:** http://www.spo.go.kr/ / Phone: 02-3480-2000
- **Police Agency, Cyber Terror Response Center:** www.ctrc.go.kr / Phone: 182

Article 11 (Rights of Users and Legal Guardians):

1. Users and legal guardians of children under the age of 14 ("children") can exercise the following rights regarding the personal information of themselves or the children:
    - Viewing and correcting personal information.
    - Withdrawing consent for the collection and use of personal information at any time.
2. Withdrawal of consent can be done:
    - Through the settings screen within the game by selecting membership withdrawal or account deletion.
    - By contacting customer service (1:1 inquiry).
    - Note: If personal information is deleted due to membership withdrawal, related information generated while using the company's game services may also be deleted.
3. When collecting personal information from children, the company obtains consent

from legal guardians. Collected guardian information is used only for verifying consent or responding to requests for viewing, correcting, or deleting children's personal information.

4. If guardians directly visit the company for requests, they may be required to present proof of their relationship with the child.
5. If the company has valid reasons to reject requests for viewing or correcting personal information, users will be notified and provided explanations.

<Supplementary Provision>

June 11, 2025