V2.07

Privacy Policy

All personal information that Korea International School (KIS) handles is collected, retained, and processed under relevant statutes or with the consent of data subjects. KIS has established the following privacy policy to protect the rights and interests of data subjects and to handle any complaints regarding personal information.

Article 1 (Purpose, Items, Retention Period)

Personal information processed by KIS based on the relevant statutes or with the consent of the data subject is as below.

Purpose	Items of Information	Retention & Use Period
Admission Assessment and Management of Student Records	Student's name, personally identifiable information, nationality, address, contact number, family details, academic records, and photos. Parent's name, personally identifiable information, nationality, contact number, and occupation	5 years after admission assessment. Semi-permanent management of student records
Health and Hygiene Management	Current medical condition and medications, blood type, medical history, vaccination records, and medical check-up records	5 years after graduation or withdrawal
Management of EE trips and Off Campus Events	Student name, birth date, health information including blood type, current medications, and medical history. Parent's name and contact number	6 months after graduation or withdrawal
Management of School Bus Riders	Student's name, address, and contact number. Parent's name and contact number	6 months after graduation or withdrawal
Security Management	Student's name, contact number. Parent's name, contact number, and vehicle plate number	6 months after graduation or withdrawal
Management of Library Members	Student's name and email address	6 months after graduation or withdrawal
Website Management and Online and Offline Promotion Activities	Student's name, photos, and videos	5 years after graduation or withdrawal

Article 2 (Provision to Third Parties)

① The personal information provided to third parties is as below:

Recipient	Purpose	Items of Information	Retention & Use Period

Catering Company	Unpaid bill claims	Student's name, Parent's contact number	6 months after graduation or withdrawal
Travel Agency, Hotel, Insurance Company	Transportation and accommodation booking, insurance sign-up	Student's name, personally identifiable information, contact number, photo, Parent's name, contact number	Upon purpose completion

② KIS handles and retains personal information only for the purposes specified in Article 1. KIS does not provide personal information collected and retained thereby, to any third party without data subject's consent, except the following cases:

a. Where a data subject specifically consents to provide his/her personal information
b. Where another statute provides expressly
c. Where it is considered necessary for the interests of the data subjects
d. Where it is impossible to obtain consent from a data subject or his/her legal representative because his/her whereabouts are unknown or he/she is unconscious
f. Where personal information is provided in a form that makes it impossible to identify a specific person, as necessary for compiling statistics or scientific research

Article 3 (Outsource Processing and Cross-border Transfer)

1. Manage Bac LLC 2. 121 SW Salmon St Ste 1200, Portland, Oregon, 97204, U.S.A. 3. Data is sent to the outsourcee platform when applying for admission. 4. support@openapply.zendesk.com 5. Student's name, personally identifiable information, address, contact number, and photos. Parent's name, personally identifiable information, contact number, and occupation 6. Data storage (for admission management purposes) 7. Five years after admission assessment	1. Maia Learning Inc. 2. 22700 Alcalde Rd. Cupertino, CA 95014 U.S.A. 3. Data is sent to the outsourcee platform when applying for a university. 4. support@maialearning.com 5. Student's name, email address, and address. Parent's name and email address 6. Data storage (for university application management purposes) 7. Five years after graduation
1. Follett School Solutions, LLC 2. 1340 Ridgeview Dr., McHenry, IL 60050, U.S.A. 3. Data is sent to the outsourcee platform when using the library for the first time. 4. privacy@Follett.com 5. Student's name, email address, and student ID number	1. PowerSchool Group LLC 2. 150 Parkshore Dr, Folsom, CA 95630 U.S.A. 3. Data is sent to the outsourcee platform upon admission. 4. Security@PowerSchool.com 5. Student's name, personally identifiable information, address, contact number, and

6. Data storage (for library member management purposes) 7. Six months after graduation or withdrawal	photos. Parent's name, personally identifiable information, contact number, and occupation 6. Data storage (for school register and academic management purposes) 7. Semi-permanent
1. Google 2. 1600 Amphitheatre Pkwy, Mountain View, CA 94043, U.S.A. 3. Data is sent to the outsourcee platform when needed. 4. Support-in@google.com 5. Student's name, student ID number, personally identifiable information, address, contact information. Parent's name and contact number 6. Data storage (for academic and administrative purposes) 7. To be destroyed after achievement of business purpose	1. Seesaw 2. 180 Montgomery St, Suite 750, San Francisco, CA 94104 USA 3. Data is sent to the outsourcee platform when using the account for the first time. 4. gdpr@seesaw.me 5. Student's name, student ID number, email address, student grade, photos, and videos 6. Data storage (for communication purposes) 7. Semi-permanent
1. CPOMS 2. Acorn Business Park Skipton North Yorkshire BD23 2UE, UK 3. Data is sent to an outsourcee platform in an encrypted format upon enrollment for storage of sensitive data 4. support@cpoms.co.uk. 5. Name and email address 6. Internal Student Safety Reporting System 7. Until the purpose of safeguarding record is no longer applicable	1. TES Online 2. Building 3, St Paul's Place, Norfolk Street, Sheffield, S1 2JE, UK 3. Data is sent to an outsourcee platform upon employment. 4. help@tes.com 5. Name and email address 6. Online Professional Development 7. Upon employment contract termination
1. SkoolSpot 2. 10 Woodbury Place, Toronto, Ontario, M8W 1Y1, Canada 3. Data is sent to an outsourcee platform in an encrypted platform for all KIS employees. 4. support@skoolspot.com 5. Name, email address, resident number, passport, children(s) data for visa and admissions purposes, address, home and mobile phone, military service, and education history 6. HR Data Management System 7. Until the purpose and use of data is achieved	1. PowerSchool Schoology 2. 150 Parkshore Dr, Folsom, CA 95630 U.S.A. 3. Data is sent to the oursource platform when using the account for the first time. 4. Security@PowerSchool.com 5. Name and email address 6. Classroom Management System 7. Upon employment contract termination
1. Atlas 2. 2. 121 SW Salmon Street, Suite 1200, Portland, OR 97204, U.S.A.	

3. Data is sent to an outsourcee platform in an encrypted format upon enrollment 4. support@onatlas.com 5. Name and emaill address 6. Curriculum Management 7. Upon employment contract termination	

(Remark) 1. Outsourcee 2. Outsourcee Location 3. Outsource Date and Method 4.Contact Information of Data Protection Officers 5. Items of Outsourced Data 6. Contents of Outsourced Duties 7. Retention and Use Period

Article 4 (Data Subject's Rights)

① A data subject can exercise the following rights:

a. Request to browse, and edit the personal information

b. Request to rectify and suspend the incorrect information

c. Request to delete

② If any data subject requested to rectify or delete his/her personal information by request form, we will complete the request and send the notification within 10 days.

Article 5 (Destruction of Personal Information)

Personal information is destroyed when the purpose has been fulfilled. The procedure of the destruction of personal information, deadline and method is as below.

1. Procedure: Personal information is moved to a separate database once the purpose has been fulfilled. In accordance with school policy and other related laws, the information is saved for a certain period and destroyed later. All information moved to the database is not used for other purposes unless enforced by the law.
2. Personal information will be destroyed within 5 days after the personal information is not required due to fulfillment of the purpose, deadline of the possession and etc.
3. Personal information as electronic files will be destroyed to be irreproducible and the paper-type files with personal information will be shredded using the shredder or be incinerated.

Article 6 (Measures to Secure Safety)

KIS has implemented the following technical, managerial, and physical measures necessary to ensure safety to prevent personal information from being lost, stolen, divulged, altered, or damaged.

1. KIS has established and implemented a data protection policy (an internal management plan) in accordance with the guidelines for measures for ensuring the safety of personal information.
2. The number of data handlers has been minimized and regular educational programs have been implemented for them.
3. Access to personal information is controlled by granting, amending, or revoking the authority to access the database system that processes personal information.

Unauthorized external access is controlled by operating firewalls and intrusion prevention systems.

4. Details on granting, amending, or revoking authority are recorded, and such records are preserved for at least six months.
5. Passwords and personally identifiable information are encoded for storage and management.
6. To prevent divulgence and damage of personal information due to hacking or computer viruses, security programs are installed, updated, and inspected periodically, and systems are installed in areas where access is controlled from outside, and they are technically and physically monitored and blocked.

Article 7 (Privacy Officer)

KIS has appointed a Privacy Officer, Data Protection Officer and a department in charge to be responsible for protecting data subjects' privacy and personal information and for gathering their opinions and handling their complaints:

Role	Privacy Officer	Data Protection Officer
Name (Position)	Younghoon Kim (Business Administrator)	Andy Kim (GA Team)
Phone Number (Email)	031-789-0510 (cpo@kis.or.kr)	031-789-0514 (dpo@kis.or.kr)

Article 8 (Gathering of Opinions and Handling of Complaints)

KIS values the opinions of the data subjects. If you have any opinions or complaints related to personal information, please contact the Chief Privacy Officer or Data Protection Officer. If you need to report or consult about other personal information infringements, please contact the institution below.

- The Privacy Complaint Center (via privacy.kisa.or.kr or at 118);
- The Supreme Prosecutors' Office High-tech and Financial Crimes Investigation Division (via www.spo.go.kr or at 1301); or
- The National Police Agency Cyber Bureau (via www.ctrc.go.kr or at 182)

Article 9 (Collection of Personal Information Using Cookies)

KIS uses cookies for the convenience of data subjects. The information we collect through cookies is IP address, visit records and etc. Data subjects have the option to accept or decline the installation of cookies and may set ther web browser to accept all cookies, alert you whenever a cookie is stored, or disable or block the storage of cookies.

※ Examples of Setting Method

·For Explorer: Tools at the top of the web browser> Internet Options> Personal Information (However, if you refuse to install cookies, it may be difficult to use some services.)

·For Chrome: Settings menu on the right side of the web browser> Display advanced settings at the bottom of the screen> Content setting button for personal information> Cookies (However, if you refuse to install cookies, it may be difficult to use some services.)

Article 10 (Policy Amendment)

If any change is made to this policy by addition, deletion, or correction due to a modification or revision in relevant laws, government policies, or the school's internal regulations, KIS will post such change on the website.

Enforcement Date January 15, 2019
Amended Date August 1, 2022
Amended Date October 1, 2023

V.3.0

Visual Data Processing Device
Operation and Management Policy

The purpose of this visual data processing device operation and management policy is the clarification of the installation purpose and operation and management method of the visual data processing device(hereinafter referred as “VDPD”) operated by KIS.

Article 1 (Base and Purpose of Installation)
The VDPD is installed and operated based on the following reasons. The collected personal visual data is not used for purposes other than installation purposes.
1. Base of Installation: Article 25 paragraph 1 of the Personal Information Protection Act
2. Purpose of Installation:
   a. Safety management of students, faculty and staff, and visitors
   b. Safety management of facilities
   c. Prevention of fire and other accidents
   d. Prevention of crime

Article 2 (Operation status)
The status of the VDPD operated by KIS is as follows.
1. Number of installations: 187
2. Installation Location: Building entrances, lobbies, corridors, soccer fields, gyms, playgrounds, parking lots, etc.
3. Recording time: 24 hours
4. Processing method: Real-time recording by the magnetic device (no sound recording function)
5. Storage Location: Control Room on B2 of Elementary School Building
6. Retention period: Within 30 days (this may vary depending on storage capacity)

Article 3 (Manager and Handler)
To protect VDPD safely and deal with related requests, the VDPD manager and VDPD handler are designated as below.
1. VDPD Manager: Kim Tae-young, Facility Team Leader 031-789-0561
2. VDPD Handler: ① Shim Youngdong, Facility Team 031-789-0565
   ② ES Associate Principal (Elizabeth Retzlaff) 031-789-0643
   ③ MS Associate Principal (Miles Carey) 031-724-5708
   ④ HS Associate Principal (Rich Melamed) 031-724-5860

Article 4 (Access Request)

A data subject can request KIS to access or confirm the existence of personal visual data only when it is clearly necessary for the urgent investigation of life, body, and property. If the data subject requests in writing to access or confirm the existence of the personal visual data, KIS will deal with the request pursuant to the relevant laws. However, KIS can reject the request and notify within 10 days of the reason for rejection as below cases.

1. In cases of serious effect on a criminal investigation, maintenance of prosecution, and a trial
2. If it is technically difficult to delete only a specific image
3. In cases where there is a high risk of infringement of the rights and interests of others
4. Where there are other justifiable reasons to reject the request

Article 5 (Measures to secure safety)

The place where personal visual data is played and viewed is designated as a restricted area and access is restricted to those who are authorized to access it. In addition, to prevent forgery and falsification of personal visual data, KIS records and manages the date of creation of personal visual data, the purpose of viewing, viewer, and date.

Article 6 (Amendment)

If any change is made to this policy by addition, deletion, or correction due to a modification or revision in relevant laws, government policies, or internal regulations, KIS will post such change on the website.

Enforcement Date January 15, 2019
Amended Date November 20, 2026

Legal Base of VDPD Operation and Management Policy

Article 1 (Base and Purpose of Installation) P25(1).1
Article 2 (Operation status) P25.2, P25(1).4
Article 3 (Manager and Handler) P25(1.-3
Article 4 (Access Request) P25(1).5, P25(1).6
Article 5 (Measures to secure safety) P25(1).7
Article 6 (Amendment) P25(1).8

(Abbreviations)
A: Personal Information Act
P: Presidential Enforcement Decree of the Personal Information Act
M: Ministry of Education Ordinance of Personal Information Act