



PRIVACY POLICY

INTRODUCTION

Ramkhamhaeng Advent International School (the “**School**”) recognizes the importance of the protection of Personal Data. Therefore, the School has issued this Privacy Policy (“**Policy**”) in order to set out the principles and guidelines generally applicable to the School’s operations in relation to Personal Data protection.

1. Scope and Purposes

- (1) This Policy sets out the principles and guidelines for the School’s operations in relation to Personal Data protection to ensure that the duties and responsibilities of the School as a Data Controller are performed in accordance with the Personal Data Protection Laws.
- (2) This Policy applies to all Processing performed within the scope and in accordance with the purposes of the School as well as to the Processing by third parties, or through third party devices or systems within the scope and in accordance with the purposes of the School.
- (3) In addition to this Policy, the School will issue internal procedures, manuals, orders, notices, guidelines, or code of practice which include details, procedures, work processes relating to Personal Data protection in order to increase the compliance with this Policy.
- (4) This Policy does not apply to the processing performed by the School’s personnel for their personal interests or family activities of such personnel, which are not related to the School’s scope and purposes.
- (5) The School will review, improve, or amend this Policy if there are any amendments, improvements, changes, or additions to Personal Data Protection Laws. The School will also review, improve, or amend internal procedure manuals, orders, notices, guidelines, or code of practice to ensure that the material statement is up-to-date and compliant with the Personal Data Protection Laws.

2. Departments Required to Comply With the Policy

All personnel in all departments of the School shall have a duty and responsibility to comply with this Policy, having a DPO (if any) and/or Compliance Team of the School to provide advice, monitor and ensure compliance with the Personal Data Protection Laws.

3. Compliance Team

The *Personal Data Protection Act Compliance Committee (DP)* is responsible for ensuring that the School, all directors, executives, and personnel comply with this Policy.

4. Principles of Personal Data Protection

The Processing shall be carried out in accordance with the following principles:

- (1) The Processing shall be lawful, fair, and transparent (lawfulness, fairness, and transparency).
- (2) The Processing shall be carried out within the scope and for specified purposes and Personal Data shall not be used or disclosed in a manner that is incompatible with the scope and purposes of the Processing (purpose limitation).
- (3) The Processing shall be limited to the extent necessary in relation to the scope and purposes of the Processing (data minimization).
- (4) Personal Data processed should be accurate and, where necessary, kept up to date (accuracy).
- (5) Personal Data shall be kept for no longer than is necessary for the Processing (storage limitation).
- (6) Personal Data shall be processed in a manner that ensures appropriate security of Personal Data (integrity and confidentiality).

5. Policy Enforcement

This Policy shall become effective on the Effective Date. All other previous internal policies, procedure manuals, orders, notices, guidelines, or code of practice not in contradiction with this Policy shall remain in full force and effect.

Effective from *June 01, 2022*, onwards.

6. **Definitions**

“Committee”	means	the Personal Data Protection Committee.
“Data Controller”	means	the data controller as defined under the Personal Data Protection Laws.
“Data Processor”	means	the data processor as defined under the Personal Data Protection Laws.
“Data Processing Agreement”	means	an agreement between the Data Controller and the Data Processor which governs the performance of obligations of the Data Processor to be in accordance with the Personal Data Protection Laws.
“Data Subject”	means	a natural person who can be identified directly or indirectly by the Personal Data (not as an owner in terms of property rights or creator of such data).
“Office”	means	the Office of the Personal Data Protection Committee.
“Personal Data”	means	the personal data as defined under the Personal Data Protection Laws.
“Personal Data Breach”	means	an unlawful or unauthorized loss, access to, use, alteration, correction, or disclosure of Personal Data.
“Processing”	means	any operation or set of operations performed upon Personal Data, whether or not by automated means, including but not limited to collection, recording, organization, structuring, storage, adaptation, alteration, receipt, review, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, and destruction.

- “Personal Data Protection Laws”** means all laws, regulations, and other legal requirements, including but not limited to the Personal Data Protection Act. B.E. 2562 (2019) and its sub-regulations issued hereunder, official guideline and interpretation thereof, as applicable to the Processing (as amended and/or replaced from time to time).
- “Sensitive Data”** means Personal Data which is sensitive and if exposed to others, would result in unfair discrimination or impact on the rights and freedoms of Data Subject, and must therefore be processed with special caution. It includes data on race, ethnic origin, political opinions, religious or philosophical beliefs, sexual behavior, criminal records, health data, disabilities, trade union information, genetic data, biometric data, and any other data as prescribed by the Committee.

CHAPTER 1

Duties and Responsibilities for Policy Compliance

1. The Personal Data Protection Act Compliance Committee (DP) shall be responsible for overseeing compliance with the Personal Data Protection Laws, acting through Compliance Team, as well as approving policies, procedure manuals, orders, notices, guidelines, or code of practice which include details, procedures and work process of a particular subject relating to Personal Data protection policies of the School.

2. All departments of the School that handle Personal Data shall have the following duties:
 - (1) attach importance to and strictly comply with the Personal Data Protection Laws, this Policy, internal procedure manuals, orders, notices, guidelines, or code of practice relating to Personal Data protection of the School.
 - (2) issue internal procedure manuals, orders, notices, guidelines, or code of practice relating to Personal Data protection to govern compliance and communicate with personnel in the department in order for them to have knowledge and understanding to correctly carry out their works according to the Personal Data Protection Laws, this Policy, internal procedure manuals, orders, notices, guidelines, or code of practice relating to Personal Data protection of the School.
 - (3) arrange for an IT system to support the operation process of Personal Data protection, that is suitable, adequate and conform to Personal Data Protection Laws, this Policy, internal procedure manuals, orders, notices, guidelines, or code of practice relating to Personal Data protection of the School.
 - (4) ensure that all personnel in the department strictly comply with this Policy, internal procedure manuals, orders, notices, guidelines, or code of practice relating to Personal Data protection of the departments.
 - (5) arrange for a Data Processing Agreement when engaging a third party to carry out the Processing by order or on behalf of the School.

3. All personnel in all departments of the School shall have the following duties:

- (1) attach importance to and strictly comply with the Personal Data Protection Laws, this Policy, internal procedure manuals, orders, notices, guidelines, or code of practice relating to Personal Data protection of the School.
- (2) attend Personal Data protection training programs as scheduled and when receive attendance notification. Personnel shall value training and commit to attend training sessions.
- (3) report any Personal Data Breach to the head of department in order to jointly conduct investigation of the incident and shall, after having become aware of it, promptly notify Compliance Team who will further notify the Office of the incident within the period prescribed by the Personal Data Protection Laws.
- (4) not disclose Personal Data of Data Subjects made known to them or obtained in the course of performance of work for other persons, unless otherwise provided by law.

4. Compliance Team shall have the following duties:

- (1) develop Personal Data protection policies of the School and propose to the authorized committee for approval.
- (2) jointly develop internal procedure manuals, orders, notices, guidelines, or code of practice relating to Personal Data protection which include details, procedures and work process of a particular subject relating to Personal Data protection policies of the School with relevant departments of the School and may propose to the authorized committee for approval.
- (3) ensure that staff, personnel, and relevant departments of the School strictly comply with Personal Data protection policies and internal procedure manuals, orders, notices, guidelines, or code of practice relating to Personal Data protection.
- (4) communicate new, updated, changed, or amended policies or regulations on Personal Data protection to personnel and relevant departments of the School for acknowledgment and compliance.
- (5) provide staff, personnel, and relevant departments of the School with advices on regulations and operations as well as training sessions on operations in relation to Personal Data protection.
- (6) serve as the point of contact between the Office and the School.

- (7) keep records of the Processing activities in a record of the Processing activities as required by Personal Data Protection Laws. Any initiation, amendment to, update or cessation of the Processing activities carried out by the department requires opinion of the DPO (if any) in the form of record of the Processing activities.
 - (8) assess risks associated with current and new Processing of the School as required by the Personal Data Protection Laws.
 - (9) conduct audits or reviews to assess the School's compliance with policy, internal procedure manuals, orders, notices, guidelines, or code of practice relating to Personal Data protection of the School.
 - (10) discuss relevant legal issues, Personal Data breach or content of any documents, agreements, or forms with the DPO (if any).
5. The Human Resources Departments (staff & academic) shall be responsible for providing support and organizing training sessions in order for new personnel and existing personnel in relevant department to have knowledge and understanding of Personal Data Protection Laws, this Policy, internal procedure manuals, orders, notices, guidelines, or code of practice relating to Personal Data protection of the School. Personnel attendance on training sessions shall be recorded. The department shall schedule training sessions for personnel when it is time to brush up on their knowledge, and manage Personal Data of directors, executives, and personnel of the School in accordance with this Policy.
6. The Information Communication Technology (ICT) Department shall be responsible for providing support and arranging for a high-performance IT system that is suitable, adequate and meets legal requirement to be implemented in Personal Data protection operation process for services, service channels or operation process of relevant departments in order to facilitate operations and ensure that operations are compliant with the Personal Data Protection Laws.

CHAPTER 2

Purposes of the Processing

The School shall comply with the Personal Data Protection Laws as follows:

1. Carry out the Processing only for clearly defined and lawful purposes such as the following:
 - 1) to perform pursuant to agreement with Data Subject or the Data Subject's wishes.
 - 2) to offer services to Data Subject and promote services of the School.
 - 3) to render services under the terms or agreements between the School and domestic or foreign vendors or contracting parties, external service providers, agents of service providers who support the School's provision of service and business partners.
 - 4) to conduct studies, researches or statistical analysis which will be used for managing business affairs of the School or to create communication materials for students and parents, vendors or contracting parties and the School's executives and personnel.
 - 5) to comply with the legislation relevant to the School's operation and future laws applicable to the School.
 - 6) to submit or disclose information and documents in support of the conduct of legal proceedings or the issuance of order by regulatory authorities or agencies with legal authority, or to comply with orders of government agencies with legitimate authority upon their request.
 - 7) to measure satisfaction of Data Subject in order to improve services.
 - 8) to manage risks and business affairs of the School according to this Policy or under the terms of agreements of the School.
 - 9) to fulfill obligations under the terms and/or employment agreements or the School's work rules between the School and directors, executives and personnel who are the Data Subjects.
 - 10) other purposes in accordance with the applicable laws.
2. Notify Data Subject of the purpose of the Processing prior to or during the collection of Personal Data via appropriate channels and means.

3. Perform the Processing only for the specific purpose of which Data Subject has been informed. The School may carry out the Processing for purposes other than the original purpose only when other lawful bases, as prescribed by the Personal Data Protection Laws, can be determined and the Data Subject was informed of a new purpose prior to or at the time of the Processing.

CHAPTER 3

Processing

In order to be compliant with the Personal Data Protection Laws, the School has set out principles of the Processing as follows:

1. At least one of the following lawful bases under the Personal Data Protection Laws must be determined for the Processing:
 - 1) It is based on the consent that had been given by the Data Subject.
 - 2) It is for the preparation of historical records for public interest, research, or statistics.
 - 3) It is for preventing or avoiding danger to life, body, or health of a person.
 - 4) It is for the performance of a contract to which the Data Subject is a party or in order to take steps at the Data Subject's request to use service prior to entering into a contract.
 - 5) It is for the performance of a task carried out in the public interest by the School or in the exercise of official authority vested in the School.
 - 6) It is for the legitimate interests pursued by the School or the Data Subject, provided that such interests do not seriously affect fundamental rights and freedoms or interests of the Data Subject and do not cause burden on or unfairness to the Data Subject.
 - 7) It is for the compliance of legal obligations of the School.
2. At least one of the following conditions under the Personal Data Protection Laws must be determined for Processing of Sensitive Data:
 - 1) It is based on the explicit consent that had been given by the Data Subject.
 - 2) It is for preventing or avoiding danger to life, body, or health of a person where the Data Subject is incapable of giving consent.
 - 3) It is carried out in the course of legitimate activities by foundations, associations, not-for-profit bodies, or trade unions with appropriate safeguards.
 - 4) It relates to data which has been made public with the Data Subject's explicit consent.

- 5) It is for the establishment of legal claims.
 - 6) It is for the compliance with a law to achieve the purposes with respect to preventive or occupational medicine, healthcare, labor protection, social security, national health security, medical welfare, scientific, historical, or statistical research, or other substantial public interests.
3. The Compliance Team shall have the authority to determine lawful bases and conditions for the Processing according to the details provided by departments performing the Processing.
 4. Personal Data shall only be directly collected from Data Subjects. Where it is necessary for the School to collect Personal Data from sources other than from the Data Subject such as public sources on a determined lawful basis, third parties e.g. vendors or contracting parties, external service providers, agents of service providers who support the School's provision of service, and business partners, departments of the School shall set out procedures and operational approach which are correct and in strict compliance with the Personal Data Protection Laws and approved by Compliance Team.
 5. Procedures for requesting consent and withdrawal of consent from Data Subjects and/or persons with parental responsibility in the case that the Processing is performed on the Data Subject who is a minor, incompetent or quasi-incompetent shall be established in accordance with the Civil and Commercial Code and the Personal Data Protection Laws.
 6. Procedures for protection of Personal Data transmitted or transferred to a foreign country or international organization shall be established. The destination country that receives such Personal Data shall have adequate data protection standards or as permitted by Personal Data Protection Laws. For the transmissions or transfers of Personal Data among affiliated businesses in a foreign country, the School shall carry out data transmissions or transfers according to Personal Data protection policy of the School which must be reviewed and certified by the Committee.
 7. Procedures for managing processed Personal Data existing prior to the Personal Data Protection Laws becoming effective shall be established.
 8. Roles, responsibilities and work procedures of the School and vendors or contracting parties, external service providers, and business partners shall be clearly determined, whether in the capacity of Data Controllers or Data Processors, to ensure that operations of vendors or contracting parties, external service providers, and business partners are in compliance with the Personal Data Protection Laws.

CHAPTER 4

Request for Consent and Withdrawal of Consent of Data Subject

In Request for order to be compliant with the Personal Data Protection Laws concerning request for Data Subject's consent, the School shall follow the following procedures:

1. Discuss with the Compliance Team in order to draw conclusions about the necessity and content of request for consent for the Processing.
2. Where consent is required, the School shall state the purpose of the Processing and any other data as required by law when requesting consent from Data Subject prior to or during the Processing.
3. Request for consent shall comply with the following requirements:
 - 1) The request for consent shall clearly state the purpose of the Processing and not be made in a manner that is deceptive or misleading to the Data Subject.
 - 2) The statement requesting for consent shall be presented in a manner which is clearly distinguishable from other matters and shall not be bundled up as part of an agreement or terms and conditions of service.
 - 3) The request shall be made using clear and plain language.
 - 4) The consent must be freely given by the Data Subject.
 - 5) The request for consent may be made in writing or electronically unless it is by nature impossible to be made by such means.
 - 6) The Data Subject is able to refuse or withdraw his or her consent at any time on his or her initiative.
4. Channels for Data Subject to give or withdraw consent shall be properly provided, either via electronic means or contacting personnel, agents, or third parties acting on the School's behalf. Such channels shall not unfairly discriminate or place constraints on the Data Subject who is a socially disadvantaged person or person with disability.
5. Procedures for withdrawal of consent shall be established and shared to the Data Subject who has given consent to the School. It shall be easy to withdraw consent and the Data Subject shall be informed of the likely consequences of withdrawal of consent.
6. Procedures for requesting consent and withdrawal of consent from Data Subjects and/or persons with parental responsibility in the case that the Processing is performed on the Data Subject who is a minor, incompetent or quasi-incompetent

shall be established in accordance with the Civil and Commercial Code and the Personal Data Protection Laws.

7. A central Consent Management System of the School shall be set up to effectively manage the process of giving and withdrawing consent of Data Subjects. Departments of the School shall have their relevant IT systems connected to such systems or set up a process to record the requests for consent and withdrawal of consent to be incorporated into such systems and shall ensure that requests for consent and withdrawal of consent are always recorded.

CHAPTER 5

Privacy Notice

The School recognizes the importance of the protection of Personal Data of Data Subjects. Therefore, the School have set out the guidelines of privacy notice as follows:

1. Procedures and methods for notification of privacy notice shall be established to provide the Data Subject with the details of the School's Processing prior to or at the time of collection of Personal Data.
2. Privacy notice shall include at least the following information as prescribed by the Personal Data Protection Laws:
 - 1) Purpose and lawful bases for the Processing.
 - 2) Personal Data collected and retention period for Personal Data.
 - 3) Sources of Personal Data such as collected directly from the Data Subject or from other reliable sources.
 - 4) Persons or authorities to whom Personal Data may be disclosed.
 - 5) Contact details and how to contact the School, its representatives or its DPO (if any).
 - 6) Data Subject's rights according to the Personal Data Protection Laws.
3. Privacy notice may be made in writing or electronically depending on the suitability.
4. There shall be proper channels for publishing privacy notice, either electronically or via contacting personnel, agents or third parties acting on the School's behalf which shall ensure that Data Subject is informed of the School's privacy notice prior to or at the time of Personal Data collection.

The School may provide privacy notice through a variety of the following media: (1) orally - face to face or when personnel in the School speak to the relevant person on the telephone (the School must document such case); (2) in writing - printed media, printed adverts, forms, such as admission forms or job application forms; (3) through signage – e.g. an information poster in a public area for the use of CCTV; and (4) electronically - on the School's websites or in emails. The aforementioned channels may be adjusted from time to time as the School deems appropriate.

5. Update or revise privacy notice to reflect the School's actual and up-to-date Processing. Periodically review details of privacy notice and record all updates or changes to the privacy notice which are to be used as evidence for inspection.

CHAPTER 6

Retention and Retention Period for Personal Data

The principles of retention and retention period for Personal Data are as follows:

1. Retention Period

The School shall retain Personal Data for only as long as it is necessary for the purposes it is required for the Processing until the end of the Data Subject's relationship with the School. However, the School may need to retain Personal Data for longer periods as required by law or the School's policy or regulations to achieve a specific purpose. Retention periods will differ among sections and specific data.

2. Data Retention Procedure

The School may retain Personal Data in original, copy or electronic format or in other forms which can be converted into a document for use as evidence and made available for inspection and submission upon the request of the Office.

The School shall delete or destroy Personal Data according to the principles for erasure or destruction of Personal Data when it is no longer required for the purpose of the Processing or after the retention period has ended or in other circumstances required by the Personal Data Protection Laws.

CHAPTER 7

Erasure or Destruction of Personal Data

The principles of erasure or destruction of Personal Data are as follows:

1. There shall be a system or measure to detect if one of the following grounds applies in order to carry out erasure or destruction of Personal Data:
 - 1) The Personal Data is no longer necessary to be retained in relation to the purposes for which it was processed.
 - 2) The Data Subject withdraws consent on which the Processing is based, and the School has no legal ground for the Processing.
 - 3) The Data Subject objects to the Processing and the School cannot reject the Data Subject's request to exercise his or her right.
 - 4) The Processing was unlawful.
2. Methods for erasing or destroying Personal data

The School shall erase, destroy, or anonymize Personal Data of the Data Subject according to the Personal Data Protection Laws.

CHAPTER 8

Security Measures for Personal Data

In order to ensure that Personal Data is properly and effectively protected in accordance with the Personal Data Protection Laws, the School shall carry out the following activities:

1. Put data security measures in place to protect Personal Data either stored in IT system or otherwise such as documents containing Personal Data, to prevent Personal Data Breach.
2. Establish effective, appropriate security measures according to the requirements of Personal Data Protection Laws; and
3. Conduct reviews of the security measures if there are updates, changes, modification to the School's principles or when there are new legislation under the Personal Data Protection Laws or any updates, changes, amendments thereto, or any relevant legislation is implemented, in order to ensure appropriate and adequate security measures for Personal Data.

The School shall also record how the Personal Data is handled, whether in a hard copy or electronic format, providing details as required by the Personal Data Protection Laws and made available for inspection by Data Subject and the Office.

CHAPTER 9

Measures Facilitating the Exercise of Rights of Data Subject

Since the School recognizes the importance of the rights of the Data Subject, the School has set out the following measures to facilitate the exercise of rights of the Data Subject in accordance with the Personal Data Protection Laws:

1. The rights of Data Subjects under the Personal Data Protection Laws are as follows:
 - 1) Right to withdraw consent.
 - 2) Right to access and obtain a copy of Personal Data and right to request disclosure of the Personal Data obtained without consent.
 - 3) Right to data portability.
 - 4) Right to object to the Processing.
 - 5) Right to erasure, destruction, or anonymization.
 - 6) Right to restriction of the Processing.
 - 7) Right to rectification of Personal Data; and
 - 8) Right to lodge a complaint.
2. A channel for submission of a request to exercise the rights of Data Subject shall be established to facilitate the Data subject in exercising his or her rights.
3. A department serving as a central unit shall be established to handle the Data Subject's request to exercise his or her rights.
4. Time periods for responding to the Data Subject's request to exercise his or her rights and for notifying the Data Subject without undue delay of the decision made on the request shall be determined.
5. In the event that the School refuses the Data Subject's request, records of such refusal together with the reasons of refusal and the specific Processing activities that has been refused shall be kept as evidence for inspection when requested by the Office or the Data Subject.

CHAPTER 10

Personal Data Breach Notification

In the event of a Personal Data Breach, the DPO (if any) or Compliance Team shall take the following actions:

1. Investigate the circumstances of the Personal Data Breach in order to implement appropriate measures to mitigate the impact and prevent future breaches.
2. The DPO (if any) or Compliance Team shall notify the Data Subject and the Office of the Personal Data Breach based on the situation and the extent of the incident as required by laws in accordance with the following guidelines:

Impact on the rights and freedom of Data Subject	Actions to be taken
There is no risk	- Record Personal Data Breach
There is a risk	- Record Personal Data Breach - Notify the Office within 72 hours
There is a high risk	- Record Personal Data Breach - Notify the Office within 72 hours - Notify the Data Subject of Personal Data Breach and remedial action as soon as possible

3. In the case where the IT system or relevant operation fails to function, the personnel or department who discovers an incident shall notify the IT system within 48 hours after having become aware of it. The IT system shall coordinate with the DPO (if any) or Compliance Team to take appropriate steps.
4. In case of other incidents associated with Personal Data Breach, the personnel or department who discovers an incident shall directly notify DPO (if any) or Compliance Team as soon as possible to take appropriate steps.

CHAPTER 11

Data Protection Officer

In the case where the School has a duty under the Personal Data Protection Laws to designate a data protection officer (“**DPO**”), the School must:

1. Appoint a DPO based on expert knowledge of Personal Data Protection Laws and the ability to perform his or her duties independently.
2. Inform the Office of the appointment of the DPO together with other information as required by the Data Protection Laws within the timeframe as specified by the Data Protection Laws; and
3. Provide the DPO with adequate tools or equipment as well as facilitate access to the Personal Data in order for the DPO to perform his or her duties.

The DPO shall have the following duties:

1. Conduct monitoring and inspection of compliance with this Policy, internal procedure manuals, orders, notices, guidelines, or code of practice to ensure that the School’s Processing complies with the Personal Data Protection Laws.
2. Provide advice to departments and personnel of the School concerning compliance with this Policy.
3. Coordinate and cooperate with the Office on issues regarding the Processing by the School and the Schools’ personnel in compliance with this Policy.
4. Maintain confidentiality of Personal Data known or acquired in the course of performance of his or her duties under this Policy.
5. Report issues associated with performance of his or her duties under this Policy to the executive authorized committee.
6. Support and provide assistance in impact assessment of Personal Data protection of departments.
7. Provide consultation on Personal Data protection and serve as the point of contact for Data Subject as well as handle complaints and requests and carry out matters related to the exercise of rights of Data Subject.
8. Monitor and resolve complaints about Personal Data protection.
9. Keep records of Personal Data Breach and notify the Office as required by Personal Data Protection Laws.

10. Document opinions on matters relating to the School's Processing.
11. Serve as the point of contact of the School for matters regarding the School's Processing; and
12. Perform other tasks as assigned pursuant to this Policy.

CHAPTER 12

Internal Audit for Personal Data Protection

The School shall procure an internal audit of the adequacy of the procedures and measures of Personal Data protection in order to demonstrate whether the School is meeting its obligations under the Personal Data Protection laws. The internal audit procedures are set out below.

1. The internal audit shall be performed independently.
2. Performance assessment shall be carried out to measure the procedures and measures in operation in relation to Personal Data protection in the whole School at least once a year.
3. The results of such audit shall be directly reported to the DPO (if any), Compliance Team and/or the authorized committee. In the case where weaknesses or issues in operations of relevant departments are identified and found to be non-compliant with the Personal Data Protection Laws, the executives and personnel of such relevant departments shall promptly make improvements and corrections according to the audit results, including requesting relevant approval from the relevant authorized personnel of the School for any amendment of any procedures, measures, and documents.

CHAPTER 13

Training on Personal Data Protection

The School recognizes the importance of personnel training which provides personnel with knowledge and understanding of the operating procedure of Personal Data protection to prevent Personal Data Breach or any incidents that are not in compliance with the Personal Data Protection Laws. Guidelines for personnel training on Personal Data protection are as follows:

1. All new personnel shall receive basic training on Personal Data protection before commencement of employment or whenever it can be ensured that the new recruits have taken and passed such basic training, in this regard, there should be post-tests given to personnel after training sessions to measure knowledge gained and records of training on each particular subject shall be kept as evidence.
2. Existing personnel shall receive training to brush up on their knowledge on Personal Data protection regularly, at least once a year.
3. Personnel training on Personal Data protection may be conducted in a traditional face-to-face environment or using e-learning methods.

CHAPTER 14

Bring Your Own Devices Measures

In the case where the School allows the personnel to use their own devices, such as smartphones, laptops and external hard drives, for the Processing, the School shall apply the following measures to protect the security of the School's data.

Allowed Devices

1. Smartphones.
2. Laptops; and
3. External hard drives.

Acceptable Use

1. The School allows the use of the personnel's own devices that directly or indirectly support the Processing.
2. Devices may not be used at any time to:
 - Deliberately propagate a virus, malware, or any other malicious program code.
 - Access, use or disclose confidential information without authority; and
 - Violate any applicable laws, including the Personal Data Protection Laws.

Security

1. In order to prevent unauthorized access, devices must apply authentication, e.g. a strong and appropriate password to access the School's data.
2. The personnel's data and the School's data should be stored separately. Personnel should not inadvertently or deliberately move the School's data into their personal storage on the devices or onto separate personally owned devices.
3. Passwords are recommended to be changed every 90 days and should be a unique new password every time.
4. Once the password has been set by the personnel, it must be kept confidential.
5. The devices such as smartphones and laptops should lock itself with a password if it's idle for 5-10 minutes.

6. The personnel access to the School's data shall be limited based on user profiles defined by the School and automatically enforced.
7. The personnel must keep the software (including the operating system) up to date at all times.
8. The use of external hard drives must be registered with the School and the external hard drives must be securely kept in order to avoid unlawful loss, access, use, alteration, correction, or disclosure of Personal Data contained in such external hard drives.
9. Lost or stolen devices must be reported to the School within 72 hours.

Deletion when off-boarding

When the personnel off-boarding, the School will wipe the School's data on the personnel's device and/or software, require the personnel to submit their device for review before leaving and delete or deactivate the authorized account.

CHAPTER 15

Sensitive Data in a Copy of National ID Card

In the case where visitors exchange national ID cards for visitors' cards before entering into the School's building and premises, the security guards should only record the necessary personal data into the logbook, such as full name and national ID card number, in order to prevent the unnecessary collection of sensitive data in a national ID card.

Related Policies and Documents

- *all documents*

Communication

- *Orientations with students and parents*
- *School Website*
- *Student Handbook*
- *Teachers' Handbook*
- *Posters*
- *QR Codes*

Policy Review Cycle

- This policy will be reviewed once every three years.
- This policy was last reviewed by RDOC in November 2023.