ICS Policy on the Personal Data Protection Act (PDPA)

Introduction

The International Community School (ICS) will, in the process of its operations; collect, process, disclose and use personal data in compliance with the requirements of Thailand's Personal Data Protection Act (PDPA) and according to the guidelines in this policy.

The Basics

“Personal data” includes any data pertaining to a living natural person that enables the identification of that person, whether directly or indirectly. The PDPA applies to both digital and physical data, and includes information such as phone numbers, addresses, email addresses, or anything that might enable identification of the data subject—the person directly or indirectly linked to the information in question.

Types of information collected:

- Personal details and demographic information (name, contact details, gender, nationality, medical information, passports, national ID, etc. (for students and families as needed)
- Financial information (only when applying for tuition assistance at ICS)
- Normal work history, education history, references, contact and family information of employees
- Responses to surveys
- Text, images, and film from school-related activities
- Inquiries and comments via the ICS website and social media

Purpose of data collection:

- Maintain regular communication channels for communicating student progress and disseminating information regarding school programs
- Administration and intervention in the event of medical or pastoral counseling requirements
- Review strategic plans, academic policies and guidelines
- Management of security and risk
- Provide education services, track progression of students and evaluate student’s suitability for a course
- Regulatory reporting and compliance
- Analysis of information to improve and develop the ICS website
- To ensure student health and safety

- To apply for and maintain legal status in Thailand
- To determine the need for financial assistance
- To make enrollment decisions or for the purpose of assigning placement in certain activities or services
- To supply data to other schools or universities at the request of the student or parents
- To respond to an inquiry via the website or other channels
- To establish the suitability of an employment applicant and application of benefits of the candidate, if hired

Confidentiality of Information

Authorized personnel within ICS and appointed data intermediaries will be able to access the information you provide to us. We only do so with your consent and will always ensure that your information is used in accordance with the terms of this privacy policy and the Thailand PDPA. Unless required or permitted to do so by law, we will not otherwise share, sell or distribute any of the information you provide to us without your consent.

How to contact us

The confidentiality of your personal data is important to ICS. You have our assurance that if your personal data is collected, used or disclosed for the purposes we have listed above, we will use it only in accordance with the Thailand Personal Data Protection Act (2019) requirements. If you need clarifications, corrections, access to your information, withdrawal of consent for use of your personal data, or other information regarding your personal data kept with ICS, you can contact the school office at: +662-338-0777

The following is more in-depth explanation of this policy and the Thailand PDPA

PDPA Main Roles

The PDPA lays out three main roles relating to the handling of others' personal data: the data controller, the data processor, and data protection officer. The data controller is a person or entity with power to make decisions regarding collection, use, and disclosure of personal data. The data processor is a person or entity that collects, uses, or discloses personal data on behalf of, or under the instructions of, the data controller. The data controller carries significant liability and obligations, while the processor's obligations and liabilities are very limited in comparison.

Data controller's obligations

Data controllers take principal responsibility for ensuring that ICS staff fulfill all their obligations for handling personal data, including collection, use, and transfer. Their first duty is to ensure that throughout these steps, the personal data remains correct, up-to-date, complete, and not

misleading. In terms of security and maintenance, the data controller must implement suitable measures for preventing loss, unauthorized access, alteration, or disclosure of personal data. These measures must be reviewed whenever necessary, such as after the implementation of technological developments. The data must be recorded in a form, either written or electronic, that can be inspected by the data subject or an authorized party. When the storage period expires, the personal data is no longer relevant or exceeds the scope of necessity, or the consent is withdrawn. The data controller then is also responsible for seeing that the personal data is erased. At ICS, this person, the school superintendent, is inevitably responsible for this, but is assisted by members of the leadership team and various members of the ICS administrative staff.

Data processors' obligations

Data processors are required to strictly comply with the controller's lawful instructions and orders, and conversely not take action outside those instructions. The data processor must also implement suitable measures for preventing loss or unauthorized access. They must make sure suitable measures for storing personal data and preventing unauthorized access are in place. The data processor must also record processing information. This means maintaining an inventory of the collection, transfer, and use of personal data. At ICS, data processors are all of those who imput, access and use the data as listed above and include nurses, finance office staff, the registrar, the admissions staff, IT staff, teachers, web developers, and various other administrative staff.

Data Protection Officer

Data controllers or processors with a large amount of personal data will also have to appoint a data protection officer (DPO) to monitor and verify compliance with the PDPA by conducting compliance audits or inspections. The DPO will interact with the regulator if any issues arise. Businesses with a large retail customer base that generates a large volume of personal data will probably already have a DPO in place. The PDPA requires appointment of a DPO if the nature of the data controller's activities consist of collecting, using, and disclosing personal data, or if these activities require monitoring due to the large scale of personal data (the exact scale to be set later by the Personal Data Protection Commission). At ICS we will not have a specific Data Protection Officer, rather this function is also the responsibility of the superintendent.

<u>Collecting consent</u>

The collector of personal data must either have **consent** from the data subject or be covered by one of the exemptions detailed below. Consent can be given in writing or in electronic form. A request for consent must be clear and must not be deceptive or cause the data subject to misunderstand. The controller seeking consent must inform the data subject of the purpose of collection; the type of personal data being collected; relevant third parties to whom the data will

be disclosed; and the period of retention or use. Any changes to this information will require further consent, and consent can be withdrawn at any time.

Some exceptions, such as when the personal information is for educational, research, or statistics collection purposes (provided appropriate personal data protection measures are in place), or when it helps to prevent danger to a person's life, body, or health. Also, certain contractual obligations do not require further consent. For instance, an agreement to sell goods and deliver them to various locations or email addresses would not need consent for handling each separate delivery address or email.

Data subjects' rights

Under the PDPA, data subjects are accorded a number of rights over their personal data:

1. Objection: The right to object to any collection, use, or disclosure of personal data at any time.
2. Access: The right to ask a data controller to provide a copy of the data subject's personal information and disclose where they obtained it. The data controller will now be obligated to disclose, upon request, how they obtained the data subject's personal data.
3. Erasure: The right to ask a controller to anonymize or delete personal information at any time.
4. Data portability: The right to obtain the data in commonly used machine-readable format. This right lets a data subject, for example, ask a hospital to transfer all personal data to the subject or to another hospital.

ICS PDPA Adherence Statement

The below will be located at the conclusion of every form of data collection we have at ICS including but not limited to ICS Student Applications, ICS Teacher Applications, Tuition Assistance Applications, online after school enrichment sign-up forms, online camp/sport/field trip sign-up forms, etc.

By checking this box, you affirm that you have read and understand the ICS Personal Data Protection Policy and hereby agree to submit and grant access to your personal data to ICS based on the guidelines set out for collecting, use of, and retention of that information as well as the rights afforded to you by this policy and the Thailand PDPA.