Content

Title：	Implementation Regulations Governing Personal Information File Security Maintenance Planning in Overseas Taiwan Schools and in Schools for the Children of Businesspeople from Taiwan in the Mainland Area Ch
Date：	2016.09.01
Legislative：	1.Ministry of Education Order No. Tai-Jiao-Wen-(2)-1050115002B issued on 1 September 2016 Full text of all articles

Content：

Article 1

These Regulations have been formulated in accordance with the provisions of Paragraph 3 of Article 27 of the Personal Information Protection Act (hereunder abbreviated to "the Act").

Article 2

The competent authority referred to in these Regulations is the Ministry of Education.

Article 3

The following terms used in these Regulations are defined below:

1. "Personal information manager" (hereunder abbreviated to "manager") refers to the person who is responsible for supervising the formulation and implementation of the personal information file security maintenance plan (hereunder referred to as "data security plan"). This will be the school principal, or a person appointed by the principal.
2. "Personal information auditor" (hereunder abbreviated to "auditor") refers to the person assigned by the school principal to be responsible for evaluating the implementation and effectiveness of the data security plan.
3. "Employee" refers to any staff member of the school who must access personal information during the course of undertaking their work. This term includes staff members on fixed-term and non-fixed-term contracts and temporary personnel.

The manager referred to in Subparagraph 1 of the preceding paragraph and the auditor referred to in Subparagraph 2 of the preceding paragraph are not permitted to be the same person.

Article 4

Overseas Taiwan schools established in accordance with the Regulations for the Establishment and Assistance of Overseas Taiwan Schools, and schools in the Mainland Area for the children of businesspeople from Taiwan established in accordance with the Regulations for the Establishment and Assistance of Mainland Area Schools for the Children of Businesspeople from Taiwan (hereunder collectively referred to as "offshore Taiwan schools") shall each formulate a data security plan and implement the maintenance and management of personal information file security, to prevent the theft, alteration, damage, loss, or disclosure of personal information.

The plan referred to in the preceding paragraph shall include the method(s) for dealing with personal information if an offshore Taiwan school ceases its operations, as a matter related to the management of personal information.

Article 5

When an offshore Taiwan school formulates its data security plan, it shall formulate appropriate security maintenance measures, taking into account its scope and the

nature and quantity of the personal information it retains.

Article 6

An offshore Taiwan school shall complete the formulation of its data security plan within one year from the day after the date that these Regulations are promulgated and take effect, and report this to the competent authority for future reference.

Article 7

An offshore Taiwan school may designate or set up a management unit, or designate a particular person, to be responsible for personal information file security maintenance. The duties of this unit or person are as follows:

1. Formulate and implement the data security plan, including the method(s) for dealing with personal information after the school terminates its operations.
2. Submit regular written reports to the manager regarding the status of the school's personal information file security maintenance and management.
3. Carry out reviews and make improvements, based on the auditor's evaluation of the implementation of the data security plan, and then submit a written report to the manager and to the auditor.

Article 8

An offshore Taiwan school shall confirm that it has specific designated purposes for the collection of personal information and, based on what is necessary in order to meet these specific purposes, delineate the categories and scope of the collection, handling, and use of personal information, and thoroughly re-examine the status of the personal information that it is retaining at regular intervals.

If, during the course of a regular inspection, an offshore Taiwan school discovers that it has personal information that is outside the scope necessary for the designated purposes, or that the designated purposes no longer exist, or that the time limit has expired and there is no longer any necessity to retain it, the school shall delete or destroy such personal information, or take other appropriate measures to cease its collection, handling, or use.

Article 9

When an offshore Taiwan school collects personal information, it shall check whether the information is within the categories and scope stipulated in Paragraph 1 of the preceding article.

When an offshore Taiwan school transmits personal information, it shall adopt the protection measures necessary to avoid disclosure of that personal information.

Article 10

An offshore Taiwan school shall analyze and assess the possible risks that could arise, based on the defined scope of the personal information and on its processes for collecting, handling, and using such information, and formulate appropriate control measures.

Article 11

When an offshore Taiwan school collects personal information, it shall comply with the provisions of Article 8 and Article 9 of the Act related to the duty of notification. It shall also categorize the personal information into directly collected and indirectly collected information, and formulate separate methods, content, and other matters for attention regarding any notifications for information in each category, and it shall require its employees to duly apply these.

Article 12

If an offshore Taiwan school uses personal information for publicity, promotion, or marketing purposes, it shall specifically inform the person(s) whose information it is of the registered name of the offshore Taiwan school and the source of their personal information.

The first time that an offshore Taiwan school uses personal information for publicity, promotion, or marketing purposes, it shall provide the person(s) whose information it is with a means of indicating that they decline to agree to the use of their personal information for any publicity, promotion, or marketing, and the school shall pay any necessary expenses. If a person indicates that they decline to permit their personal information to be used for any publicity, promotion, or marketing, the school shall immediately cease any use of any of the person's personal information for publicity, promotion, or marketing, and it shall inform all of its employees to do so.

Article 13

When an offshore Taiwan school authorizes any other person to collect, handle, or use all or part of the personal information it has, in accordance with the provisions of Article 8 of the Enforcement Rules of the Act, it shall exercise appropriate supervision of any such authorized person and clearly stipulate any related supervision matters and the method of supervision.

Article 14

When a person whose information is held by an offshore Taiwan school exercises a right in accordance with the provisions of Article 3 of the Act, the school may adopt the following means to handle the matter:

1. Provide a contact window and contact method.
2. Verify whether the person contacting the school is the person whose personal information it is, or whether they have been authorized by the person whose personal information it is.
3. If any grounds exist on which an exercise of rights by a person whose information an offshore Taiwan school has may be refused in accordance with the proviso to Article 10, or the provisos to Paragraph 2 or Paragraph 3 of Article 11, of the Act, notify the person and attach a copy of the reason.
4. Inform the person whether the offshore Taiwan school will charge any fee for necessary costs and of the fee-charging criteria, and comply with the time limits for handling the matter stipulated in Article 13 of the Act.

Article 15

An offshore Taiwan school shall formulate a response mechanism to use if any theft, disclosure, alteration, or other infringement of personal information occurs, to handle the matter rapidly and protect the rights and interests of the person(s) whose information it is.

The response mechanism referred to in the preceding paragraph shall include the following:

1. Appropriate measures to be taken to control the harm or loss that such an incident has caused or could cause the person(s) whose information it is.
2. Investigation to ascertain the cause of the incident and the damage caused, and notification of the person(s) whose information it is by appropriate means.
3. Consideration of measures for improvement, to avoid any recurrence of such an incident.

An offshore Taiwan school shall notify the competent authority within three days from the date that it discovers that any incident referred to in Paragraph 1 has occurred, and within one month from the date that it has finished dealing with the matter, the school

shall submit a report of how it handled the matter and the result to the competent authority for future reference.

Article 16

An offshore Taiwan school shall install the necessary security equipment and adopt the necessary precautionary measures for the personal information files it is retaining.

The security equipment or precautionary measures referred to in the preceding paragraph shall include the following:

1. Security protection installations and management procedures for hard-copies of data files.
2. Associated equipment such as computers or automated machinery used to store electronic data files, and the deployment of security and protection systems and/or encryption mechanisms.
3. Formulation of procedures for the destruction of hard copies of data. When any computer, automated machinery, or other storage medium used for storing personal information needs to be written off, replaced, or used for another purpose, the school shall adopt appropriate preventative measures to avoid any disclosure of personal information.

Article 17

In order to ensure the safeguarding of the security of personal information, an offshore Taiwan school shall adopt the following measures regarding its employees:

1. In accordance with the operational requirements of the school, set up a management mechanism, and delineate the authority of individual employees, in order to control and manage the nature of access each has to personal information. Regularly re-ascertain whether the current delegations of authority are appropriate and necessary.
2. Review the nature of all related operations, and establish protocols governing the collection, handling, and use of personal information for the personnel responsible.
3. Require employees to handle and store personal information storage media in a proper way, and stipulate employees' associated handling, storage and confidentiality responsibilities and duties.
4. When an employee of an offshore Taiwan school leaves employment, the school shall cancel their identifier and shall require the departing employee to hand over all personal information that they were holding for undertaking their work (including hard-copy and storage media versions). The departing employee is not permitted to take or use any such information and shall sign a non-disclosure agreement.

Article 18

An offshore Taiwan school shall formulate a mechanism for auditing its personal information file security maintenance and conduct inspections of the implementation of its data security plan regularly, or from time to time, then submit a report of the findings of the inspection to the manager.

The staff member who undertakes the audits referred to in the preceding paragraph and the person responsible for personal information file security maintenance referred to in Article 7 are not permitted to be the same person.

The offshore Taiwan school shall incorporate the auditing mechanism referred to in Paragraph 1 into its internal control and audit items.

Article 19

When an offshore Taiwan school is implementing each of the procedures and measures of its data security plan, it shall keep records of at least the following:

1. Handing over and transmission of personal information.
2. Maintenance, revision, deletion, destruction, or transfer of personal information.

3. Provision of the exercise of related rights by persons whose information is held.
4. Records of access to the personal information system.
5. Backup and recovery testing.
6. Changes to delegated authority of any employee.
7. Breaches of authority by any employee.
8. Measures adopted in response to any incident that has occurred.
9. Regular checking of the information system that handles personal data.
10. Education and training.
11. Implementation of data security plan audits and improvement measures.
12. Records of data disposal after an offshore Taiwan school terminates its business operations.

Article 20

Regarding the collection, handling, and use of personal information, an offshore Taiwan school shall provide education and training or awareness programs for its employees regularly, or from time to time, to ensure that they clearly understand the provisions of the ordinances related to the protection of personal information, their areas of responsibility, operational procedures, and related measures that they must comply with.

Article 21

After an offshore Taiwan school terminates its operations, the method(s) for disposing of the personal information it has been retaining and the records to be kept are as follows:

1. Destruction: The method, time, and location of the destruction of personal information, and the method of certifying its destruction.
2. Transfer: The reason, content, method, time, and location of the transfer, and the legal basis on which the party receiving the personal information is permitted to receive and retain it.
3. Other deletion, or cessation of the handling or use of personal information: The method, time, and location of the deletion or the cessation of the handling or use.

Article 22

An offshore Taiwan school shall monitor whether the data security plan it formulated continues to be appropriate, taking into consideration the actual implementation of its data security plan, technological developments, and any amendments to the ordinances which constitute its legal basis, and it shall revise the plan when necessary.

Article 23

These Regulations shall take effect on the date of promulgation.

Data Source： Laws and Regulations Retrieving System