NSYSU Office of Student Affairs Regulations for Student Personal Data Management

History of Amendment and Approval:
9th Student Affairs Division Meeting of 2010-Academic Year (1st semester) on 30-12-2010
2nd Student Affairs Meeting of 2010-Academic Year on 14-01-2011

Article 1 In order to protect the privacy of student personal data, prevent personality infringement and ensure the completeness and rightful usage of student personal data, the Office of Student Affairs (hereinafter referred to as the Office) stipulates these Regulations.

Article 2 The student personal data mentioned in the Regulations include: student status, counseling data, commandment and sanction, health data, and other student related data established from administrative affairs.

Article 3 The Office proceeds and protects personal data carefully in accordance to the Personal Data Protection Act and other related laws, while also executing personal data safety maintenance, data entry, and storage. Management principles are divided into operational personnel management and information system usage management according to how data are established and kept.

Article 4 Operational personnel management principle:

All personal data of students recorded or saved by operating personnel of the Office due to administrative affairs shall be promptly kept and maintained with a devised safety protocols to protect the data from theft, tampering, destruction, loss or disclosure.

Operating personnel of the Office must not disclose any data of related students or their families without written consent of related parties or in accordance to a request by law.

Article 5 Information system usage management principle:

The usage principles of the information system (information platform) of the Office are as follows:

(1) Accounts are to be logged out immediately after using or retrieving student personal data related files. Keeping the account in a state where the data can be viewed or modified is forbidden.

(2) Accounts and passwords of the system are not to be used by anyone other than the actual account owner. In cases where the computer and other equipment undergo updates or maintenance, the account owner is not to notify the manufacturer of the account and password. Instead the account owner must log into the account before temporarily letting the manufacturer perform the maintenance or update.

(3) Authorized operating personnel must not disclose any data related to students or their families without written consent of related parties.

(4) Authorized operating personnel must pay attention to safety protection of the machines at all times to prevent data getting leaked through whichever possible methods.

Authorization and application of user permission for the information system (information platform) of the Office

(1) The main system administrator of the platform should be the information personnel from or appointed by the Office and is in charge of managing permissions and user authorization of the platform.

(2) System administrator duties are carried out by operational personnel from each system in principle.

(3) For the user authorization and account opening of the platform, except from when the system is first introduced and multiple accounts are created by the administrator, other departments can request authorization based on administrative needs. Accounts will be opened upon review from system administrators. User accounts will automatically become void when the account owner is no longer in the University.

(4) Student authorization for the platform: All currently enrolled students of the University can log in.

(5) Instructor authorization for the platform: all current instructors of the University can log in. Mentor authorizations are updated by the system based on the mentor student list of the semester.

Article 6 The regulation is passed by the Student Affairs Division Meeting and implemented upon approval by the Student Affairs Meeting. The same procedure applies in cases of amendments.