NTU STUDENT LEADERS
Compliance with the Personal Data Protection Act (PDPA)

General
The PDPA governs the collection, use, disclosure and care of personal data in Singapore by organisations. It recognises both the rights of individuals to protect their personal data, including rights of access and correction, and the needs of organisations to collect, use or disclose personal data for legitimate and reasonable purposes.

Every student organisation, as data user who controls the collection, holding, processing, disclosure, transfer or use of personal data, has to observe the personal data privacy rights of an individual.

What is Personal Data?
Personal data refers to data, whether true or not, about an individual who can be identified from that data; or from that data and other information to which the organisation has or is likely to have access.

The term “personal data” should be interpreted broadly, and covers all types of data from which an individual can be identified.

Examples:
Full Name, Residential Address, Mobile Number, NRIC/Passport Number, Matriculation Number, Bank Account Details, Personal Image etc.

Do Not Call (DNC) Registry Provision
The DNC regime under the PDPA does not allow organisations to call, fax or send marketing messages to Singapore telephone numbers without explicit consent. This is also applicable to smartphone applications that use a telephone number as an identifier, such as WhatsApp or Line, as long as the specified message is addressed to a Singapore telephone number.

For more information, please refer to the DNC Advisory Guidelines.
Data Protection Provision
The Data Protection Provisions set out the obligations that organisations are required to comply with if they undertake activities relating to the collection, use or disclosure of personal data.

Points to observe for all Student Organisations
- All student organisations are required to appoint at least one key personnel as a Data Protection Officer to oversee the organisation’s compliance with the PDPA. The committee list should also include this position when submitting to SAO.
- All consent given by students or the public must be obtained in writing accompanied with a comprehensive set of purposes for collection, use and disclosure of the personal data.
- It is compulsory to state a point-of-contact on your website and publicity materials to allow students and members of the public to submit requests to opt-out of marketing materials or correction to their personal data.
- All personal data must be kept accurate and up-to-date and must not be kept longer than necessary.
- Every committee member must take precautionary measures to ensure that the personal data is being kept secure from misuse and unauthorized access.
- No sharing or exchanging of personal data is allowed between student organisations unless written consent from the individual has been obtained.
- Organisations who wish to send marketing related messages via sms/phonecall/fax or via email/post should only do so after obtaining clear and unambiguous written consent from the individual.
- Use “BCC” field when mass mailing to students and members of the public to mask other recipients email address.
- Event organisers must put up notices to notify participants of the seminar or event that photographs and/or videos of them may be taken for specified reasonable purposes. (Refer to Templates for sample notification.)

Updated on 23 Nov 2015