HANG SENG MANAGEMENT COLLEGE

Policy Guidelines and Procedures
in Compliance with Personal Data (Privacy) Ordinance

I. Preamble

The Hang Seng Management College (College) respects personal data privacy and as a data user, we are fully committed to implementing and complying with the data protection principles and all relevant provisions of the Personal Data (Privacy) Ordinance (PDPO). In compliance with the Ordinance, the following policy guidelines and procedures have been prepared to provide practical guidance to staff members and students of the College on the proper handling of personal data in carrying out College functions and activities.

II. Definition of terms

In accordance with the Personal Data (Privacy) Ordinance, definition of terms used in this code is given as below:

**Personal Data** - means any data - (a) relating directly or indirectly to a living individual; (b) from which it is practicable for the identity of the individual to be directly or indirectly ascertained; and (c) in a form in which access to or processing of the data is practicable.

**Data User** – in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of the data.

**Data Subject** - relation to personal data, means the individual who is the subject of the data.

III. Data Protection Principles

All staff members and students are required to comply with all relevant provisions of the Ordinance and to adhere to the following six principles in the collection, use, storage and/or disposal of personal data:

**Principle 1 -- Purpose and manner of collection.**
This provides for the lawful and fair collection of personal data and sets out the information a data user must give to a data subject when collecting personal data from that subject.
Principle 2 – Accuracy and duration of retention.
This provides that personal data should be accurate, up-to-date and kept no longer than necessary.

Principle 3 – Use of personal data.
This provides that unless the data subject gives consent otherwise personal data should be used for the purposes for which they were collected or a directly related purpose.

Principle 4 -- Security of personal data.
This requires appropriate security measures to be applied to personal data (including data in a form in which access to or processing of the data is not practicable).

Principle 5 -- Information to be generally available.
This provides for openness by data users about the kinds of personal data they hold and the main purposes for which personal data are used.

Principle 6 – Access to personal data.
This provides for data subjects to have rights of access to and correction of their personal data.

IV. Code of Practice for Data Users

Principle 1 – Purpose and manner of collection

1.1 Personal Information Collection Statement
In collecting personal data, the data user should provide a Personal Information Collection Statement (PICS). In the PICS, the data subjects must be informed of the purposes for collecting their personal data, as well as any third parties to whom the data may be transferred, the individual’s rights to request access to and correction of their personal data and the contact of the officer to whom such requests should be made. Data subject should be informed whether or not it is obligatory for them to supply the data and the consequences of not providing such data.

1.2 Manner of Data Collection
In collecting personal data, the data user should ensure that the personal data will only be collected for a lawful purpose, and by lawful and fair means. Also, the data user should ensure that the personal data collected in relation to a specified purpose must be adequate but not excessive in respect of the purpose.
Principle 2 – Accuracy and Duration of retention

2.1 Data retention

Before collecting personal data, the data user should first of all consider and decide on the duration of retention and notify the data subjects accordingly. If the personal data collected will be kept for a period of time, mechanism must be in place to allow correction of data and to ensure accuracy of the data held.

Under the current practice, respective department/unit has set the retention period of the personal data kept by them.

2.2 Personal data should not be kept longer than necessary for the fulfillment of the purpose of which it is collected.

2.3 Data Accuracy

If the personal data will be kept for more than a year, the data user should consider the need to conduct an annual exercise to remind the data subjects of the personal data held and the importance of keeping their data up-to-date with the data user.

2.4 Data Disposal

The data user shall be responsible for ensuring that personal data no longer needed after the specified retention period should be properly disposed of (e.g. shredding), to avoid personal data being seen and/or collected by unauthorised persons.

Principle 3 – Use of Personal Data

3.1 The data user should only use the personal data for the specified purpose for which they were collected or a directly related purpose; and should not use them for other purposes; save and except that explicit consent has been obtained from the data subject.

3.2 The data user should also ensure that the personal data will not be transferred to any other parties not authorised to use the personal data; save and except that explicit consent has been obtained from the data subjects.

3.3 The “need-to-know” principle should be applied in the handling of all documents containing personal data.
Principle 4 – Security of personal data

4.1 All reasonably practicable steps should be taken to ensure that personal data held are protected against unauthorized or accidental access, processing, erasure or other use.

4.2 As a matter of good practice, personal data should be kept in confidential files locked in cabinets in a controlled area accessible only by staff authorized to handle such personal data or kept in password-controlled electronic files.

4.3 A “clear-desk” policy is required of all staff members who are given access to personal data. They must put all documents containing personal data in locked cabinets before leaving the work station for an extended period of time and at the end of each working day.

4.4 Staff or students granted access to personal data on a “need-to-know” basis should not make private copies of any such personal data or communicate with unauthorized parties within or outside the College on such personal data.

4.5 Papers containing personal data should not be re-used as “re-cycled paper” and or any other purposes. They must be properly disposed of after the retention period.

4.6 Proper deletion of personal data in computing devices and removable storage must be done before re-deploying computer equipment to a new user or dispatching these devices for maintenance or disposal.

4.7 Staff and students should adopt appropriate measures to ensure the secure transmission of personal data, e.g. data being put in a sealed envelope marked “confidential” with the addressee specified, data being encrypted or password-protected and the data recipients double-checked to ensure that they are the right data transferees during the electronic transmission.

4.8 Staff and students are not allowed to carry mobile computing devices and removable storage media containing identifiable personal data outside of the College premises. They must also make sure that these devices are securely kept and the data contained therein are properly encrypted and/or password protected.

Principle 5 - Information to be generally available

5.1 The following information in relation to personal data of the College shall be made generally available:

(a) the kinds of personal data held;
(b) the main purpose for which personal data are used; and
(c) the policies and practices in relation to personal data.

Principle 6 - Access to personal data

6.1 The data user should identify a contact person to be in charge of handling data access request from data subjects.

6.2 A data subject who wishes to make a request for access to his/her own personal data held by the data user should complete the Personal Data Access Request Form (OPS 003).

6.3 The data user can charge a fee of HK$150 for the initial search, and then a processing fee of HK$5 per page to cover the cost of photocopying.

6.4 When handling personal data access, care must be taken to provide only the personal data requested by the data subject but not the personal data of any other data subject which may be revealed in the same document.

6.5 The data user should keep and maintain a good record of data access request with inclusion of reasons of refusing to data access request (if applicable). A form in Appendix 1 can be used for that purpose.

6.6 Data Access Request Form (OPS 003)
査閱資料要求表格(OPS 003)
(http://www.pcpd.org.hk/chinese/publications/files/Dformc.pdf) can be completed and return it to the following departments/offices for action:

<table>
<thead>
<tr>
<th>Personal Data Relating to</th>
<th>Department/Unit in charge*</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Job applicants/staff members of the College</td>
<td>Human Resources Office</td>
<td><a href="mailto:hr@hsmc.edu.hk">hr@hsmc.edu.hk</a></td>
</tr>
<tr>
<td>Students of the College</td>
<td>Registry</td>
<td><a href="mailto:registry@hsmc.edu.hk">registry@hsmc.edu.hk</a></td>
</tr>
<tr>
<td>Alumni of the College</td>
<td>Alumni Affairs Office</td>
<td><a href="mailto:alumni@hsmc.edu.hk">alumni@hsmc.edu.hk</a></td>
</tr>
</tbody>
</table>

*Note: Human Resources Office, Registry and Alumni Office are the major holders of the personal data of staff, students and alumni respectively in the College. If necessary, the data access request may have to be forwarded to responsible Department/Unit for further handling.

6.7 The responsible staff who takes care of data access request will notify the data subject in writing of the outcome and/or progress of the request within 40 days from the date of submission.
V. Reporting on Loss of Personal Data

In the unfortunate event of any loss of personal data, the staff/student concerned must report the case to the Head of Department/Office; the Dean of School and then the Vice-President (Organizational Development)’s Office immediately.

A meeting will be called as soon as possible, to ascertain the seriousness of the situation, any damage likely to be caused to the data subjects, any remedial actions that need to be taken to contain and/or minimise the damage, parties to be informed and apologies to be sent to the data subjects.

In some circumstances, the police may need to be called and the Commission on Personal Data (Privacy) will need to be informed.

VI. Others

Other than the above-mentioned policy guidelines and procedures, staff and students are required to comply with all relevant provisions of the Personal Data (Privacy) Ordinance.

This policy guidelines and procedures are subject to review from time to time and may be subject to change.

VII. References:

Reference information from the website of Office the Privacy Commissioner for Personal Data has been made in the compilation of this code of practice:

Personal Data (Privacy) Ordinance Chapter 486 (Full Text)

Code of Practice on Human Resources Management (2000)

Guidance on the Use of Portable Storage Devices (2011)

Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users (2012)

22 November 2012
HANG SENG MANAGEMENT COLLEGE  
Compliance with Personal Data (Privacy) Ordinance  
Requests on Data Access - Log book

Name of Office: ________________________________

<table>
<thead>
<tr>
<th>Request No.</th>
<th>File Ref.</th>
<th>Date request received</th>
<th>Information requested</th>
<th>Name of Data Subject</th>
<th>Handled by (Reply Date)</th>
<th>In case of refusal, state reason(s) here</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>