THE HONG KONG
INSTITUTION OF ENGINEERS
香港工程師學會

Privacy Management Programme (PMP) Manual for The Hong Kong Institution of Engineers (HKIE)

Table of Contents

1. Introduction to the Privacy Management Programme ("PMP")

The Privacy Commissioner for Personal Data, Hong Kong ("PCPD" or "the Privacy Commissioner") advocates that organisational data users should embrace personal data privacy protection as part of their corporate governance responsibilities. The PCPD believes that by applying it as a business imperative throughout the organisation, covering business practices, operational procedures, service design, physical architectures and network infrastructure, everyone will benefit through having these embedded levels of protection.

The PMP is a strategic framework, which assists organisations to build robust privacy infrastructures supported by effective on-going review and monitoring processes. It also facilitates organisations to comply with the requirements under the Personal Data (Privacy) Ordinance (Cap.486) ("PDPO"). In February 2014, the PCPD issued the "Privacy Management Programme: A Best Practice Guide", which outlines good approaches for developing a PMP. The Best Practice Guide was revised in August 2018 with more concrete examples, charts, templates of questionnaire and checklist for reference[1].

In February 2014, the Hong Kong Special Administrative Region Government, together with twenty-five companies from the insurance sector, nine companies from the telecommunications sector and five organisations from other sectors, all pledged to implement PMP. Although not participating in the pledge, the Hong Kong Association of Banks has indicated to the PCPD that the banking industry supports the voluntary PMP and individual banks will take necessary steps having regard to their own privacy protection framework to implement the principles of PMP.

This PMP Manual serves as a reference guide for The Hong Kong Institution of Engineers (HKIE) to develop and implement the PMP. This PMP Manual outlines the policies, practices, requirements and guidance relating to the handling of personal data at the HKIE.

The HKIE should follow this PMP Manual when governing the collection, processing, maintenance and disposal of personal data. Top management support is required for the successful implementation of this PMP Manual and relevant programme controls. Top management or its delegated authority should appoint corresponding responsible parties, endorse the programme controls and report to the management, as appropriate, on the programme.

Enquiries

Any enquiries regarding (i) this PMP Manual; (ii) the implementation of PMP at the HKIE and (iii) the handling of personal data at the HKIE should be addressed to the Data Protection Officer of the HKIE.

[1] https://www.pcpd.org.hk//english/resources_centre/publications/files/PMP_guide_e.pdf

2. Overview of the Personal Data (Privacy) Ordinance

Legislative Background

The PDPO was enacted in 1995 and amended in 2012. The objective of the PDPO is to protect the privacy of individuals in relation to personal data.

Key Definitions under the PDPO[2]

Personal Data

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.

Examples of personal data collected, used and/or processed at the HKIE include:

- name;
- date of birth;
- age;
- gender;
- marital status;
- telephone number;
- address;
- identity card number;
- photo;
- occupation;
- employment-related record (e.g. resume, academic qualification, performance appraisal report, conduct and discipline, training and developments, leave files, records related to salary and other fringe benefits, etc.);
- medical record;
- transaction records; and
- credit card information, etc.

Data Subject

A data subject refers to the living individual who is the subject of the personal data concerned. A deceased person is not a data subject under the PDPO.

Data User and Data Processor[3]

A data user is a person or an organisation that either alone or jointly or in common with other persons or organisations, controls the collection, holding, processing or use of personal data.

A data processor is a person who –
(a) processes personal data on behalf of another person; and
(b) does not process the data for any of the person's own purposes.

A data user is liable as the principal for the wrongful act of its authorised data processor.

[2] Section 2(1) of the PDPO.
[3] Data Protection Principle 2(4) in Schedule 1 to the PDPO.

Personal Identifier

Personal identifier means an identifier –

(a) that is assigned to an individual by a data user for the purpose of the operations of the user; and
(b) that uniquely identifies an individual in relation to the data user,

but does not include an individual's name used to identify that individual.

Example:

Company A launched a membership scheme. Company A collects an applicant's (i.e. data subject) name, contact number and email address for processing his/her membership application. The applicant is assigned with a unique membership number (i.e. personal identifier). The applicant's information may then be passed to a third party contractor (i.e. data processor) engaged by Company A to input the personal data collected into Company A's computer systems for further processing.

Data Protection Principles ("DPPs")

The six DPPs, enshrined in Schedule 1 to the PDPO, represent the normative core of the PDPO and cover the life cycle of a piece of personal data.

DPP1 – Data Collection Principle

Personal data must be collected in a lawful and fair way, for a purpose directly related to a function or an activity of the data user. Data collected should be necessary but not excessive.

Where personal data is collected from the data subject directly, all practicable steps should be taken to notify the data subjects on or before collection of the data of the purpose of data collection, and the classes of persons to whom the data may be transferred. The best practice to fulfil these requirements is to provide data subjects with a Personal Information Collection Statement ("PICS"). For details of guidelines on the preparation of a PICS, please refer to Annex A of this PMP Manual.

DPP2 – Data Accuracy and Retention Principle

All practicable steps should be taken to ensure that personal data is accurate and should not be kept for a period longer than is necessary to fulfil the purpose for which it is used, i.e. personal data should be disposed of when it is no longer required for the purpose for which it was originally collected.

DPP3 – Data Use Principle

Personal data should only be used for the purpose for which the data is collected or for a directly related purpose, unless the data user obtains from the data subject voluntary and explicit consent to use the data for a new purpose.

DPP4 – Data Security Principle

A data user needs to take all practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.

DPP5 – Openness Principle

A data user should take all practicable steps to make known to the public its personal data policies and practices, kinds of personal data it holds and the purposes for which the data is or is to be used.

DPP6 – Data Access and Correction Principle

A data subject has the right to (i) request access to his/her own personal data held by a data user, and (ii) request the correction of the personal data supplied in a data access request if it is inaccurate. For Data Access and Correction Policy of the HKIE, please refer to Annex B of this PMP Manual.

Exemption

In general, the above six DPPs should be followed. However, there are specific cases where the PDPO provides exemption. For example, personal data held for the purpose of prevention and detection of a crime may be exempt from the provisions in respect of data access request (DPP6) and restrictions on the use of personal data (DPP3). For details of exemptions granted, please refer to Part 8 of the PDPO.

Contraventions of the PDPO

Contravention of DPPs

Contravention of DPPs does not directly constitute a criminal offence. The Privacy Commissioner may serve an Enforcement Notice to direct the data user to remedy the contravention.

Offences relating to Enforcement Notices

However, non-compliance with the Enforcement Notice is an offence and the data user is liable –
(a) on a first conviction –
    i. to a fine at level 5, i.e. $50,000 and imprisonment for 2 years; and
    ii. if the offence continues after the conviction, to a daily penalty of $1,000; and
(b) on a second or subsequent conviction –
    i. to a fine at level 6, i.e. $100,000 and imprisonment for 2 years; and
    ii. if the offence continues after the conviction, to a daily penalty of $2,000. [4]

Contraventions of the provisions under the PDPO

Contraventions of certain provisions under the PDPO are criminal offences. Examples include unauthorised disclosure of personal data without a data user's consent, non-compliance with data access requests or data correction requests, the use of personal data in direct marketing activities, failure to erase personal data no longer required and failure to comply with requirements of the Privacy Commissioner. Details of the relevant provisions are elaborated below.

[4] Section 50A(1) of the PDPO.

- ***Unauthorised disclosure of personal data***

A person will commit an offence if he/she discloses any personal data of a data subject obtained from a data user without the data user's consent, with the intention –

(a) to obtain gain in money or other property, whether for the benefit of the person or another person; or
(b) to cause loss in money or other property to the data subject.[5]

A person will also commit an offence if he/she discloses, irrespective of his/her intent, any personal data of a data subject obtained from a data user without the data user's consent, and such disclosure causes psychological harm to the data subject.[6]

The maximum penalty of committing the above offences is a fine of $1 million and imprisonment for 5 years.

- ***Non-compliance with data access requests or data correction requests***

Upon receiving a data access request, a data user is required to supply a copy of the requested data to the requestor within 40 calendar (not working) days, unless under the circumstances allowed by the PDPO[7].

A data subject is entitled to make a data correction request after being supplied with his/her personal data by a data user pursuant to a data access request.

Upon receiving a data correction request, the data user should make the necessary correction and supply a copy of the corrected data to the requestor within 40 calendar (not working) days, unless under the circumstances allowed by the PDPO[8].

Failure to handle a data access request or a data correction request in accordance with the requirements under the PDPO without reasonable excuse may constitute an offence and render the offender liable on conviction to a fine at level 3, i.e. $10,000[9].

- ***Use of personal data in direct marketing activities in contravention of Part 6A of the PDPO***[10]

Under the PDPO, a data user is required to notify the data subjects and obtain their consents before using their personal data for direct marketing purposes, or transferring such data to a third party for direct marketing purposes. A data user is also required to comply with a data subject's request, if so made, to cease to use his/her personal data in direct marketing.

Contravention of the above-mentioned direct marketing requirements is punishable by a fine of up to $500,000 and imprisonment for 3 years. If the personal data is provided to a third party for its use in direct marketing in exchange for gain, the maximum penalty is a fine of $1 million and imprisonment for 5 years. For details of the direct marketing requirements under the PDPO, please refer to the "New Guidance on Direct Marketing" issued by the PCPD[11].

---

[5] Section 64(1) of the PDPO.
[6] Section 64(2) of the PDPO.
[7] Sections 20 and 28(5) of the PDPO.
[8] Section 24 of the PDPO.
[9] Section 64A of the PDPO.
[10] Part 6A of the PDPO.
[11] The Guidance Note can be found at https://www.pcpd.org.hk/english/publications/files/GN_DM_e.pdf

-
- ***Failure to erase personal data no longer required***

Section 26 of the PDPO provides that a data user must take all practicable steps to erase personal data held when the data is no longer required for the purpose for which it was used, unless any such erasure is prohibited under any law or it is in the public interest not to have the data erased.

Contravention of section 26 of the PDPO is an offence and offender is liable on conviction to a fine at level 3, i.e. $10,000[12].

- ***Failure to comply with requirements of the Privacy Commissioner***[13]

When the Privacy Commissioner or a person designated by the Privacy Commissioner performs his/her functions or exercises his/her powers in relation to inspection and investigation under the PDPO, a person will commit an offence if he/she:

(a) without lawful excuse, obstructs, hinders or resists the Privacy Commissioner or the person designated by the Privacy Commissioner in performing such functions or exercising such powers of the Privacy Commissioner;

(b) without lawful excuse, fails to comply with any lawful requirement of the Privacy Commissioner or the person designated by the Privacy Commissioner; or

(c) provides statements which the person knows to be false or does not believe to be true or knowingly misleads the Privacy Commissioner or the person designated by the Privacy Commissioner.

The maximum penalty of committing the stated offence is a fine at level 3 i.e. $10,000, and imprisonment for 6 months.

[12] Section 64A of the PDPO.
[13] Section 50B of the PDPO.

3. The PMP of The HKIE

This PMP consists of two parts. Part A outlines the baseline fundamentals or components of creating a PMP, including (i) organisational commitment to have an internal governance structure in place that fosters a culture respectful of privacy; and (ii) programme controls, which are the components required for an effective governance structure.

Part B of the PMP discusses how to maintain and improve a PMP on an ongoing basis. A PMP should never be considered as a finished product. It requires ongoing assessment and revision in order to be effective and relevant. The components should be regularly monitored, assessed and updated accordingly to keep pace with changes both within and outside the HKIE. This may encompass changes in areas such as technology, law and best practices.

Part A – Baseline Fundamentals

A-1a. Roles and Responsibilities of the Data Protection Officer and Other Officers Assisting in the Implementation of PMP

The following staff members will assist in the implementation and management of the PMP: –

<table>
<tr><th>Role</th><th colspan="2">Responsible Staff</th></tr>
<tr><td>Data Protection Officer</td><td colspan="2">Director</td></tr>
<tr><td>Personal Data Privacy Officer</td><td colspan="2">Senior Executive Manager – Professional Services & ERB Affairs</td></tr>
<tr><td rowspan="15">Section Coordinator</td><td>Section</td><td>Responsible Staff</td></tr>
<tr><td>Accreditation & Registration</td><td>Executive Manager – Professional Standards (1)
Executive Manager – Professional Standards (3)</td></tr>
<tr><td>Conference & Function</td><td>Executive Manager – Conference & Function</td></tr>
<tr><td>Corporate Communications</td><td>Executive Manager – Corporate Communications</td></tr>
<tr><td>Division & Special Affairs</td><td>Executive Manager – Division & Special Affairs</td></tr>
<tr><td>External Qualifications</td><td>Executive Manager – Professional Standards (2)</td></tr>
<tr><td>Finance & Administration</td><td>Senior Executive Manager – Finance & Administration</td></tr>
<tr><td>Information Technology</td><td>Executive Manager – Information Technology</td></tr>
<tr><td>Institutional Affairs</td><td>Executive Manager – Institutional Affairs</td></tr>
<tr><td>Learned Society</td><td>Senior Executive Manager – Learned Society</td></tr>
<tr><td>Membership</td><td>Executive Manager – Membership</td></tr>
<tr><td>Planning & Programme Development</td><td>Executive Manager – Planning & Programme Development</td></tr>
<tr><td>Professional Services & ERB Affairs</td><td>Executive Manager – Professional Services & ERB Affairs</td></tr>
<tr><td>Training & Development</td><td>Executive Manager – Training & Development</td></tr>
</table>

Roles and Responsibilities of the staff members

The respective roles and responsibilities of the appointed staff members are as follows:

Data Protection Officer

The Data Protection Officer should manage the implementation of the PMP and facilitate the HKIE's compliance with the PDPO. He/she should also represent the HKIE in the event of an enquiry, an inspection or an investigation by the Privacy Commissioner and/or other law enforcement agencies (e.g. the Hong Kong Police Force). His/her responsibilities include:

(1) establishing and implementing the PMP programme controls, in particular –
- keeping a record of the HKIE's **personal data inventory**; initiating and monitoring the annual personal data inventory review exercise (for details of the steps to be taken, please refer to Section 3 – Part A – 2a of this PMP Manual);
- initiating and selecting Sections to participate in the **periodic risk assessment** and reviewing the completed risk assessment questionnaire (for details of the steps to be taken, please refer to Section 3 – Part A – 2c – (a) of this PMP Manual);
- monitoring, reviewing and providing advice on conducting **privacy impact assessments ("PIA")** in the HKIE (for details of the steps to be taken, please refer to Section 3 – Part A – 2c – (b) of this PMP Manual);
- carrying out **training and education** within the HKIE and promoting staff awareness on privacy protection by circulating updates on data privacy policies, guidelines and other privacy-related information (for details of the training and education plan, please refer to Section 3 – Part A – 2d of this PMP Manual);
- coordinating and monitoring the handling of **data breach incidents**; providing advice to Sections on conducting investigations and post-incident reviews (for details of the steps to be taken, please refer to Section 3 – Part A – 2e of this PMP Manual);
- providing advice to Sections on **data processor management** and carrying out data processor management review (for details of data processor management, please refer to Section 3 – Part A – 2f of this PMP Manual);
- circulating the **PMP Manual and other prevailing data privacy policies and guidelines** to staff on a half-yearly basis (for details of communication of personal data policies and practices, please refer to Section 3 – Part A – 2g of this PMP Manual); and
- monitoring, reviewing and providing advice on the **preparation of Personal Information Collection Statement ("PICS")** before a PICS is presented to an individual for collecting his/her personal data(for details on the preparation of PICS, please refer to Annex A of this PMP Manual);

(2) reviewing the effectiveness of the PMP and revising the programme controls where necessary, in particular –
- preparing the HKIE's **oversight and review plan for the PMP** and carrying out reviews according to the oversight and review plan (for details of the oversight and review plan, please refer to Section 3 – Part B – 1 of this PMP Manual); and
- conducting **annual review of the effectiveness of the PMP**; revising and updating the PMP and the relevant programme controls based on the assessment result (for details of the review checklist, please refer to Section 3 – Part B – 2 of this PMP Manual).

Personal Data Privacy Officer

The Personal Data Privacy Officer should assist the Data Protection Officer in performing his/her tasks regarding the implementation of the PMP in the HKIE. His/her responsibilities include:

- handling **privacy complaints or enquiries** to the HKIE in relation to personal data or PMP (for details of complaints handling, please refer to the Annex D of this PMP Manual); and
- handling **data access or correction requests** made to the HKIE under the PDPO (for details of the steps to be taken, please refer to Annex B of this PMP Manual).

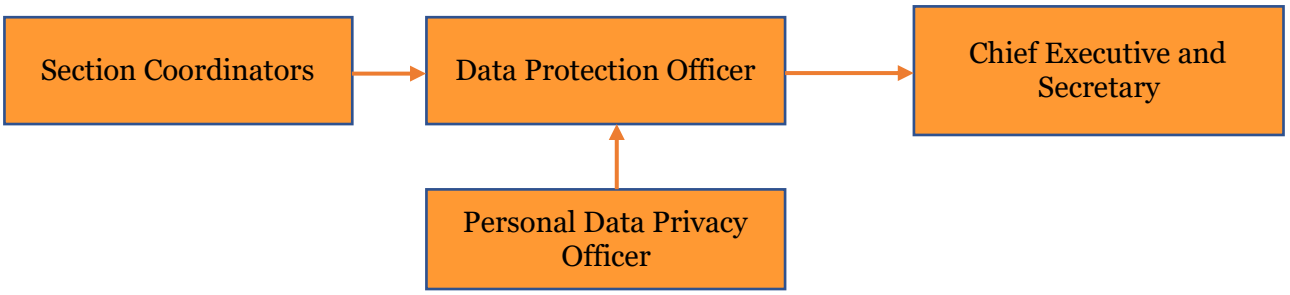
Section Coordinators

The Section Coordinators should manage the implementation of the PMP within their respective Section, and represent their respective Section to communicate with the Data Protection Officer for matters related to the PMP. Their responsibilities include:

- conducting the annual review of the **personal data inventory** of their respective Section and submitting the updated personal data inventory to the Data Protection Officer (for details of the steps to be taken, please refer to Section 3 – Part A – 2a of this PMP Manual);
- carrying out **periodic risk assessments** within their respective Section by completing the **risk assessment questionnaire**, and submitting the questionnaire result to the Data Protection Officer (for details of the steps to be taken, please refer to Section 3 – Part A – 2c – (a) of this PMP Manual);
- conducting **data processors management review** for their respective Section by completing the Data Processor Review Checklist and submitting the completed checklist to the Data Protection Officer (for details of the data processor review checklist, please refer to Annex E of this PMP Manual);
- completing the **checklist for preparation of PICS** and submitting the completed checklist to the Data Protection Officer before a PICS is presented to an individual for collecting his/her personal data (for details of the checklist, please refer to Annex A of this PMP Manual); and
- assisting the Data Protection Officer in carrying out the **Ongoing Assessment and Revision** (for details of the steps to be taken when performing the Ongoing Assessment and Revision, please refer to Section 3 – Part B of this PMP Manual).

A-1b. Reporting Mechanism

With regard to the roles and responsibilities of the staff members appointed to assist in the implementation of the PMP as described, the general reporting structure of those staff members is as follow:



The HKIE has also established specific reporting mechanisms with respect to **data breach handling**. For details of the steps to be taken, please refer to Section 3 – Part A – 2e of this PMP Manual.

2. Programme Controls

A-2a. Personal Data Inventory

The HKIE collects, holds, processes and uses different types of personal data. The HKIE should be clear about:

- what kinds of personal data its holds and where it is held and document its assessment; and
- why it is collecting, using or disclosing personal data and document these reasons.

The Data Protection Officer is responsible for maintaining a personal data inventory, which covers relevant details of all personal data the HKIE holds. A sample of the personal data inventory is included in Annex F of this PMP Manual.

Personal Data Inventory Review Exercise

To maintain an up-to-date personal data inventory, a personal data inventory review exercise should be conducted **annually**. There are five required steps when performing the personal data inventory review exercise:

Step 1 – Initiate the review exercise (Action by Data Protection Officer)

The Data Protection Officer should initiate the exercise by requesting Section Coordinators to review and update the entries in the personal data inventory under the purviews of their respective Sections.

Step 2 – Review the personal data inventory (Action by Section Coordinators)

Upon receipt of a request from the Data Protection Officer, Section Coordinators should conduct the annual review of the personal data inventory for their respective Sections with inputs from other staff members of their Sections, and update the personal data inventory as appropriate and keep track of retention period of the personal data. Section Coordinators should ensure that all types of records containing personal data held by their respective Sections are included in the personal data inventory.

The Section Coordinators shall identify any time-expired records during the review process by referring to Annex G and Annex H for “Personal Data Records Disposal Guideline” and “Records Disposal Form” respectively.

Step 3 – Submit the updated personal data inventory to the Data Protection Officer (Action by Section Coordinators)

Section Coordinators should submit the updated personal data inventory for their respective Sections to the Data Protection Officer for review and consolidation.

Step 4 – Review and finalise the updated personal data inventory (Action by Data Protection Officer)

The Data Protection Officer should review the updated personal data inventory submitted by the Section Coordinators and seek clarification or further information from the Section Coordinators when necessary, to ensure information contained in the personal data inventory is clear. When no further clarification or information is required, the updated personal data inventory can be finalised.

Step 5 – File the updated personal data inventory (Action by Data Protection Officer)

Once the updated personal data inventory is finalised, the Data Protection Officer should file the updated personal data inventory for record. The Data Protection Officer should ensure that the updated personal data inventory covers all personal data held by the HKIE.

A-2b. Policies for Handling Personal Data

The HKIE established various policies and guidelines to fulfil requirements under the six DPPs of the PDPO:

DPP1 - Collection of personal data

When collecting personal data, the HKIE must satisfy itself that –

(i) the purposes for which the data is collected are lawful and directly related to a function or activity of the HKIE;

(ii) the manner of collection is lawful and fair in the circumstances of the case; and

(iii) the personal data collected is necessary but not excessive for the purpose(s) for which it is collected.

On or before the collection of personal data from an individual (i.e. the data subject), The HKIE should always provide the data subject with a PICS in writing. For the development of PICS, the subject officers may refer to Guidelines on the Preparation of PICS at Annex A.

Handling personal data obtained over the phone

The Guidelines for Handling of Personal Data Obtained over the Phone should be adhered to. For details, please refer to Annex I.)

Collection of copies of Hong Kong Identity Card ("HKID Card")

According to the Code of Practice on the Identity Card Number and other Personal Identifiers issued by the Privacy Commissioner, unless authorised by law, no data user may compulsorily require an individual to furnish a copy of his identity card. The HKIE is not permitted to collect a copy of the identity card of an individual merely to safeguard against any clerical error recording the name or identity card number of the individual. As a result, copies of HKID Card should not be made as a mandatory item unless authorised by law. For details, please refer to Annex J.)

DPP2 - Accuracy and retention of personal data

Personal data collected and maintained by the HKIE should be as accurate, complete, and up-to-date as is necessary for the purpose for which it is to be used. The HKIE should maintain an up-to-date personal data inventory to monitor and keep track of the retention period of records that contain personal data.

All Sections should arrange to dispose of records containing personal data in accordance with the guidelines and procedures, where appropriate.

Personal data in electronic records should also be deleted immediately when there is no longer an operational need to retain the data.

If the HKIE engages a data processor, the HKIE must adopt contractual or other means to prevent any personal data transferred to the data processor from being kept longer than is necessary. For details of data processor management, please refer to Section 3 – Part A – 2f of this PMP Manual.

DPP3 - Use of personal data

All personal data collected should be used solely for the purposes which are directly related to the discharge of the HKIE's functions. Personal data collected may only be transferred to third parties during the discharge of the HKIE's functions when necessary. Relevant personal data may also be disclosed to other entities, which are authorised to receive information for the purposes of law enforcement, prosecution or review of decisions. Data subjects must be informed of the possible transferees of their personal data when their personal data is collected.

If personal data is to be used for a purpose other than the purposes for which the data is collected, express prior consent preferred in writing should be sought from the data subject concerned. In seeking the data subject's consent, all practicable steps must be taken to ensure that (i) information provided to the data subject is clearly understandable and readable; and (ii) the data subject is informed that he/she is entitled to withhold or withdraw his/her consent subsequently by giving notice in writing.

DPP4 - Security of personal data

The HKIE takes practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use. All staff handling personal data should strictly observe relevant security guidelines and regulations of the HKIE/individual Sections, and implement, where appropriate, the security measures listed below to safeguard personal data –

(i) restriction of access to personal data on a 'need-to-know' basis;
(ii) regular review and enhancement of security measures for protection of personal data in the servers, user computers, BYOD (i.e. Bring Your Own Device) and transmission of electronic messages, etc.;
(iii) regular change of passwords for IT facilities, accounting and personnel systems, etc.;
(iv) paper documents containing personal data must be stored in locked/secured location with limited access to authorised staff;
(v) limited staff access rights to office areas storing confidential information;
(vi) provision of clear guidelines to staff as to the types of data that may or may not be disclosed to a phone enquirer and implementation of appropriate identity verification procedures to confirm the enquirer's identity;
(vii) adoption of contractual or other means to prevent unauthorised or accidental access, processing, erasure, loss or use of personal data transferred to data processors (including cloud service providers);
(viii) adoption of password protecting and encrypting files to ensure that only the *receiver* with the password can access the file;
(ix) adoption of hashing with salt measure to ensure that sensitive values cannot be *seen* or *reasonably recovered* in the event of a compromise;
(x) adoption of field-level encryption to ensure that sensitive values cannot be *seen* in the event of a compromise. It involves encrypting specific data fields to hide the true value. The underlying technique of field-level encryption achieves the same function as tokenisation, but is applied to different elements in the database (i.e. identifiers vs attributes). The technical implementation of field-level encryption uses a *mathematical encryption function* instead of a *lookup table* for tokenization;
(xi) adoption of obfuscation/masking/removal of entity attributes to ensure that the exact sensitive values cannot be *seen* or *ever recovered* in the event of a compromise, although approximate or noisy values might still be seen. This involves hiding the true value of the attributes by adding noise, banding the data, or masking out portions of the value. Attributes not relevant for data usage should be removed;

(xii) adoption of dataset partitioning (of entities or attributes) to ensure that information on selected entities or attributes will not be compromised even if the larger database has been compromised. This could include protected personnel or sensitive attributes. This is done be breaking a dataset into smaller datasets by segmenting out select entities or attributes;

In addition, all electronic files containing personal data should be stored in the Section's shared drive as far as practicable. If creating or saving electronic files containing personal data in the local drive of a personal computer is required, such electronic files should be password protected.

Policy on storing personal or classified data on a portable electronic storage device

Staff should not store personal or classified data on a portable electronic storage device or remove the device from the HKIE's office without proper prior approval. Approval should only be given under exceptional circumstances with compelling operational needs. Such approval should only be granted by a supervisor at the Section Head level. For details of the application for temporary storage of classified and/or personal data on a portable electronic storage device or provision of IT devices, please refer to Annex K of this PMP Manual.

Policy on safeguarding of electronic files containing personal data, see Annex L; Policy on safeguarding of hardcopy documents containing personal data, see Annex M.

DPP5 - Transparency of the personal data policy and practices

The HKIE should take all reasonably practicable steps to make its personal data policies and practices known to the public.

Privacy Policy Statement is available for public access at the HKIE's website.

All complaints and enquiries regarding personal data privacy policy and practices or the HKIE's compliance with the PDPO should be addressed to the respective Section of the HKIE by email or by post.

The respective Section should handle the complaints and enquiries relating to personal data protection in accordance with the HKIE's established complaints and enquiries handling procedure.

A data subject may make a data correction request to the HKIE in writing or via the specified online platform. A sample of the **Personal Data Correction Request Form** is enclosed in Annex C for reference.

DPP6 - Access to and correction of personal data

An individual has the right to (i) request access to his/her own personal data held by the HKIE, and (ii) request the correction of the personal data supplied in a data access request if it is inaccurate.

For details of handling such requests, please refer to Annex B of this PMP Manual.

A-2c. Risk Assessment Tools

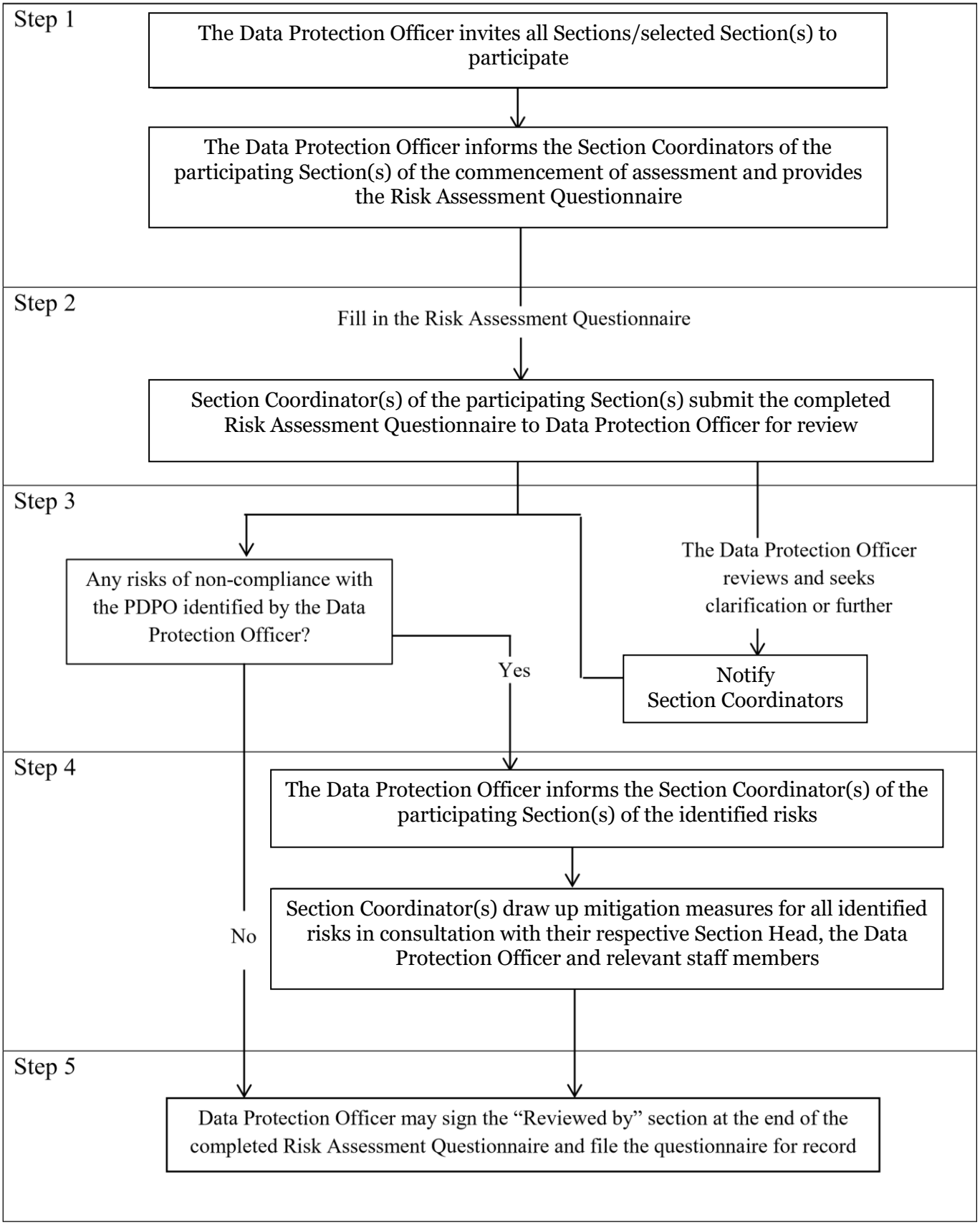
It is an important part of the PMP to ensure that the policies and practices of the HKIE are and remain compliant with the PDPO. In view of this, both **periodic risk assessments** and **privacy impact assessments ("PIA")** should be performed to assess whether the HKIE's handling of personal data is aligned with the requirements under the PDPO, and whether there are potential material changes in the handling of personal data that could lead to potential data privacy risks.

(a) Periodic risk assessment

Conducting periodic risk assessments is an important part of the PMP to ensure that the policies and practices of the HKIE are and remain compliant with the PDPO.

Every year, the Data Protection Officer should invite *all Sections/selected Sections* to participate in the periodic risk assessment. The assessment should be conducted based on the following steps:

Steps of periodic risk assessment



Step 1 – Initiate the risk assessment and invite all/select the participating Sections (Action by Data Protection Officer)

The Data Protection Officer should initiate the assessment and invite all/to select Sections to participate in the periodic risk assessment.

In selecting the Sections to participate in the periodic risk assessment, the Data Protection Officer should consider the following:

- A Section should participate in the periodic risk assessment at least once every 3 years;
- If a Section holds a large amount of personal data, its risk assessment should be conducted at least annually; and
- If a Section has changes/incidents that involve the handling of personal data, such as new initiatives launched, new data processors engaged, data breach incidents occurred or complaints received, etc., it should be selected in the year that the changes/incidents occur, or in the following year.

The Data Protection Officer should inform the Section Coordinators of every Section of the commencement of assessment / the selection result and provide the selected Sections with the Risk Assessment Questionnaire (for details of the questionnaire, please refer to Annex O).

Step 2 – Complete the Risk Assessment Questionnaire (Action by Section Coordinators)

Section Coordinators of the selected Sections should complete the Risk Assessment Questionnaire, and submit the completed questionnaire to the Data Protection Officer for review.

Step 3 – Review the Risk Assessment Questionnaire (Action by Data Protection Officer)

The Data Protection Officer should review the Risk Assessment Questionnaires submitted by the Section Coordinators.

The Data Protection Officer should then identify whether there are any risks of non-compliance with the PDPO. If any risk areas are identified, he/she should inform and seek clarification from the respective Section Coordinators and proceed to Step 4. If no risk is identified, the Data Protection Officer should proceed to Step 5.

Step 4 – Draw up mitigation measures (Action by Section Coordinators)

After the Data Protection Officer has informed the Section Coordinators the risks identified, the concerned Section Coordinators should draw up mitigation measures in consultation with their respective Section Head, the Data Protection Officer and relevant subject officers. All risks identified should be addressed.

Step 5 – File the Risk Assessment Questionnaire (Action by Data Protection Officer)

If no risk is identified or all identified risks have been addressed, the Data Protection Officer should sign the “Reviewed by” section at the end of the Risk Assessment Questionnaire and file the questionnaire for record.

(b) PIA

A PIA is a systematic process that evaluates the personal data privacy impact of the proposed changes in the handling of personal data, such as launching a new personal data handling procedure or launching a new project with the use of personal data, with the objectives of preventing and/or minimising adverse impacts. It provides data users an early warning by identifying and detecting any potential data privacy risks associated with the proposed changes before implementation.

A PIA should be undertaken –

(1) before the implementation of a new project or a change of policies and practices that involves –
- the processing or collecting of a considerable amount of personal data by the HKIE or the data processors appointed; or
- collecting, processing, using or deleting personal data in ways that are materially different from the HKIE's existing practice; or

(2) when there is a material change to the regulatory requirements relating to personal data and corresponding changes in the handling of personal data are required.

When an officer identifies the need to conduct a PIA, the following guidelines should be observed. If there is a change in the handling of personal data or a new project is launched, but the subject officer considers that there is no need to conduct a PIA (e.g. the change is of a relatively small scale), the subject officer should ensure that such consideration is properly documented.

Guidelines on Conducting PIAs

Step 1 – Consider whether to engage professional assistance to conduct the PIA (Action by subject officer)

Before conducting a PIA, the subject officer should consider whether it should be conducted internally or by external consultants. If the proposed changes in the practices of handling personal data or the new project involves significant amount of personal data and may have significant privacy impact, the subject officer may consider engaging an external contractor for professional advice.

Below are some factors to be considered in assessing whether the PIA should be carried out internally or by external consultants –

- the size and scope of the change/project;
- the types, sensitivity and quantity of personal data involved;
- the complexity of the change/project (e.g. whether there is sharing of personal data with other parties/data processors, etc.);
- whether the change/project will involve cross-border data transfer; and
- whether the change/project will involve data sharing within the organisation or with external party.

If the subject officer decides to engage external professional assistance, he/she should be aware that personal data should not be transferred to the external contractor for conducting a PIA.

If the subject officer decides to conduct the PIA internally, he/she should proceed to Step 2.

Step 2 – Complete the PIA Questionnaire (Action by subject officer)

The subject officer should, in consultation with the respective Section Head, complete the PIA Questionnaire (for details of the questionnaire, please refer to Annex P) to identify privacy risks arising from the change/project, and develop mitigation measures addressing the identified risks. For questions on system security and controls, the subject officer may seek advice from the Information Technology Section. After completing the PIA Questionnaire, the subject officer should forward the questionnaire to the Data Protection Officer for review.

Step 3 – Review the completed PIA Questionnaire (Action by Data Protection Officer)

The Data Protection Officer should review the completed PIA Questionnaire forwarded by the subject officer and ensure proper measures and controls are designed to address the identified privacy risks. The Data Protection Officer should provide comments on the questionnaire where appropriate.

Step 4 – Finalise the PIA Questionnaire (Action by Data Protection Officer and subject officer)

If the Data Protection Officer has provided comments, the subject officer should, in consultation with his/her Team/Section Head, review the comments and amend the proposed practices of handling personal data where appropriate. After addressing the comments, the subject officer and the Data Protection Officer should agree and sign off the PIA Questionnaire as evidence of approval.

Step 5 – File the PIA documents (Action by subject officer)

The subject officer should file the PIA Questionnaire approved by the Data Protection Officer and other relevant documents and correspondence in the file of the change/ project.

For details of conducting PIA, please refer to the "Privacy Impact Assessments (PIA)" information leaflet issued by the Privacy Commissioner[14].

[14] The Information Leaflet can be found at https://www.pcpd.org.hk//english/resources_centre/publications/files/InfoLeaflet_PIA_ENG_web.pdf

A-2d. Training and Education

Continuous education and training are vital for maintaining staff awareness of the importance of data privacy. The following types of training and circulate relevant information are recommended to be provided to the HKIE's staff:

Training activities	Target audience	Timing/ Frequency	Actions to be taken by the Data Protection Officer	Target achievements
Introduction of PMP	New comers	Once a staff reports duty	• Provide new comers with this PMP Manual	• Encourage the new comers to study the materials in detail
Circulation of new/updated data privacy policies and guidelines and highlights of updates in this PMP Manual	All staff	Whenever there is any new or updated data privacy policies and guidelines or PMP Manual	• Send email notifications to staff • Upload the new policies and guidelines onto the shared drive	• Provide staff with sight of the new/updated policies and guidelines as soon as practicable
Circulation of case materials including: • Risk mitigation measures drawn up from periodic risk assessments; and Case sharing (e.g. complaints in relation to handling of personal data, data breach incident(s) of the HKIE	All staff	Half-yearly	• Send email notifications to staff • Upload the case materials onto the shared drive	• Encourage other Sections to learn from the experiences and review their current practices
Re-circulation of this PMP Manual and other data privacy policies and guidelines	All staff	Half-yearly	• By e-circulation • Upload the updated PMP Manual and other data privacy policies and guidelines to the shared drive, if any	• Remind staff of the prevailing policies to ensure privacy awareness within the HKIE

Training activities	Target audience	Timing/ Frequency	Actions to be taken by the Data Protection Officer	Target achievements
Refresher course	All staff who handle a lot of personal data	To be incorporated in refresher course	• Arrange the refresher course	• Recap of the PDPO • Data protection principles Operational needs on collection of personal data • Security of personal data • How to complete a PIA
Training course	All staff who handle a lot of personal data	When appropriate	• Notify the staff members of the availability of the course • Course enrolment	• Data protection workshop held by the PCPD

A-2e. Data Breach Handling Guidelines and Procedures

A data breach is a breach of security of personal data held by a data user, exposing the personal data to the risk of unauthorised or accidental access, processing, erasure, loss or use. Below are examples of data breaches:

- Loss of storage devices that contain personal data, e.g. notebook computers, USB flash drives, portable hard disks and paper files;
- Improper handling or accidental transmission of personal data, e.g. unauthorised disposal of files, sending personal data to a third party which is not supposed to receive the personal data;
- Information security incidents such as –
    - Database containing personal data being hacked or accessed by outsiders/staff without authorisation;
    - Leakage of personal data caused by the installation of file-sharing software in the computer, etc.; and
- Misact of the data processors, e.g. sharing of personal data by the service provider with unauthorised third parties.

Data Breach Handling Guidelines

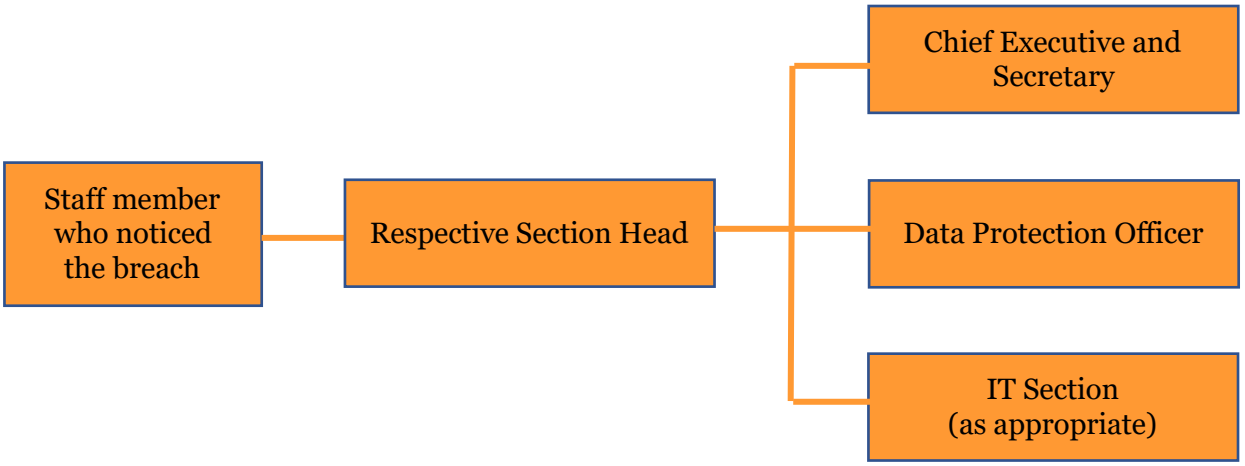
When there is a data breach or when a data breach is suspected, the respective Section should take prompt action to gather information and lessen the harm or damage that may be caused to the data subjects.

The respective Section should respond to a data breach as quickly as possible by taking the following actions.

Actions

Action – Report the breach to top management and other relevant staff members (Action by the respective Section)

A flowchart detailing the reporting structure is as follows:



When there is a data breach or a possible breach, the staff member who noticed the breach should immediately report the matter to the Section Head. The Section Head should then report the breach to the Data Protection Officer and Chief Executive and Secretary.

Action – Gather essential information relating to the breach (Action by Section Head)

The Section Head should, in consultation with the Data Protection Officer, gather the essential information about the breach and document the information in the "Information of the breach" section of the Data Breach Information Sheet (for details of the information sheet, please refer to Annex Q).

Action – Consider notifying regulatory bodies (Action by Section Head)

The Section Head should, in consultation with the Data Protection Officer, consider the circumstances of the breach and decide whether law enforcement agencies or any relevant regulators (e.g. the Hong Kong Police Force and the PCPD) should be notified.

The Section Head should complete the "Data breach notification to regulatory bodies" section of the Data Breach Information Sheet in consultation with the Data Protection Officer.

Action – Decide on the measures to contain the breach (Action by Section Head)

The Section Head should, in consultation with the Data Protection Officer, identify and adopt measures to contain the breach.

The Section Head should consider the following containment measures:

Measures applicable to the loss of portable storage devices storing personal data

- Identifying the last-known location of the concerned storage device.
- Searching for the concerned storage device to retrieve the information therein as soon as possible, if practicable.

Measures applicable to improper handling of personal data

- Suspending the improper handling of personal data, such as stopping the inappropriate delivery or disposal of documents which contain personal data.

Measures applicable to information security incidents

- Suspending the system if the data breach is caused by a system failure.
- Changing the user passwords and system configurations to control access and use.
- Ceasing or changing the access rights of individuals suspected to have committed or contributed to the data breach.
- Engaging external technical assistance to remedy the system loopholes, if necessary.
- Keeping a backup image of the affected system for investigation purpose and as evidence for subsequent follow up action.
- Assessing the impact of the incident on the concerned information system and the data contained therein.
- Protecting sensitive or critical information and systems by means such as moving the critical information to other media (or other systems) which are separated from the affected system and its relevant network.
- Shutting down or isolating the compromised computer or system temporarily to prevent further damage to other interconnected systems, in particular for incidents that will spread rapidly, for machines with sensitive information, or to prevent the compromised system from being used for launching attacks on other connected systems.

Measures applicable to the misact of data processor(s) and/or its sub-contractor(s)

- Obtaining details of the data breach from the data processor(s) and/or its sub-contractor(s).
- Requiring the data processor(s) to control the damage likely to be caused by the breach. For example, (i) ceasing or changing the access rights to the affected system of the relevant individuals whom are suspected to have committed or contributed to the data breach; (ii) enhancing the physical and/or electronic security controls at the office/site (e.g. data centre, server room) through limiting or removing the access rights to the office/site.

After deciding on the breach containment measures, the Section Head should complete the "Actions taken/will be taken to contain the breach" section of the Data Breach Information Sheet in consultation with the Data Protection Officer.

Action – Assess the risk of harm (Action by Section Head)

After deciding on the immediate actions to contain the breach, the Section Head should, in consultation with the Data Protection Officer, assess the risks associated with the breach to decide the next course of actions (e.g. should any public notification be made, should assistance be provided to affected data subjects, etc.).

The potential harm caused by a data breach may include:

- Loss of public trust
- Loss of assets (e.g. stolen computers or portable storage devices)
- Identity theft or fraud of the data subjects
- Reputational, psychological and/or material damage or loss of the data subjects
- Threat to personal safety of the data subjects

The extent of harm that may be suffered by the data subjects in a data breach depends on a number of factors, including the followings:

- The type of personal data leaked – generally the more sensitive the data is (e.g. medical record or Hong Kong Identity Card number), the greater the damage it may cause to the data subjects;
- The amount of personal data involved – generally the greater the amount of personal data leaked, the more serious the consequences can be;
- The circumstances of the data breach – in case of online data leakage, it is usually difficult to prevent further dissemination and use of the leaked personal data. However, if the recipients/destinations of the leaked data is known and traceable, the data breach may be easier to contain;
- The likelihood of identity theft or fraud – sometimes the leaked data itself or when combined with other data could facilitate identity theft or fraud;
- Whether the leaked data is adequately encrypted, anonymised or otherwise rendered inaccessible – if the leaked data is not adequately protected, the potential harm would be greater;
- Whether the breach is an isolated incident or caused by a wider problem – if the breach is caused by a wider problem (e.g. the email server has been hacked), this may continue to jeopardise the security of personal data held by the HKIE or cause further harm to the data subjects;
- In case of a physical loss (e.g. the loss of storage device or hardcopy files that contains personal data), whether the personal data has been retrieved before being accessed or copied – if the personal data has been retrieved before any limited opportunity for unauthorised access, the risk of harm would be lower;
- Whether containment measures taken are effective to stop further leakage of personal data – if containment measures taken are not effective and the breach of data cannot be stopped, it may cause more harm to the data subjects concerned; and
- The ability of the data subjects to avoid or mitigate the possible harm – the risk of harm may be lower if the data subjects are able to avoid the possible harm (e.g. if the data subjects are able to completely remove his/her personal data immediately after the data breach incident, the risk of harm would be lower).

The Section Head should complete the “Risk of harm” section of the Data Breach Information Sheet in consultation with the Data Protection Officer.

Action – Consider notifying the data subjects affected by the breach (Action by Section Head)

Having assessed the situation and the risk of harm of the data breach, the Section Head should, in consultation with the Data Protection Officer, consider issuing to the data subjects affected by the breach a **data breach notification**. Although it is not mandatory for the HKIE as a data user to notify data subjects about the data breach, the consequences of failing to give notification (e.g. the impact on the HKIE's reputation and losing public trust) should be duly considered. If the Section Head, in consultation with the Data Protection Officer, decides to issue a data breach notification, such notification should be issued as soon as practicable, except where law enforcement agencies have made a request for a delay for investigation purposes.

A data breach notification to data subjects should include the following information:

- A general description of what occurred;
- The date and time of the breach, and its duration (if applicable);
- The date and time the breach was discovered;
- The source of the breach (either by the HKIE itself or the third party that processed the personal data);
- The types of personal data involved;
- An assessment of the risk of harm caused to the data subjects by the breach;
- A description of the measures already taken or to be taken to contain the breach;
  Information and advice on actions the data subjects can take to protect themselves from the adverse effects of the breach and against identity theft or fraud;
- The contact information of the Data Protection Officer for further information and assistance; and
- Whether the Hong Kong Police Force, the PCPD or other parties have been notified of the breach.

The notification to data subjects can be made by phone, in writing, via email or in person. When data subjects cannot be identified immediately or where public interest exists, public notification through media such as the HKIE's website or press release may be more effective.

The Section Head should document the analysis by completing the "Data breach notifications to data subjects affected" section of the Data Breach Information Sheet in consultation with the Data Protection Officer.

Action – Investigate into the data breach and report the investigation results (Action by Section Head and Data Protection Officer)

After the data breach is under control, the Section Head should, in consultation with the Data Protection Officer, conduct an investigation into the breach to find out the root cause(s) of the breach and identify if the breach is related to an information system security problem, the personal data handling process or human error.

Throughout the investigation, the Data Protection Officer should assist the Section Head in coordinating with different parties involved in the data breach. When the investigation is completed, the Section Head should report the investigation results to Chief Executive and Secretary as soon as practicable.

The Section Head should document the investigation results by completing the "Investigation results" section of the Data Breach Information Sheet in consultation with the Data Protection Officer.

Action – Conduct post incident review (Action by Data Protection Officer)

The Data Protection Officer should review the Data Breach Information Sheet submitted by the Section Head, and should seek clarification or further information when necessary, to ensure information on the Information Sheet is accurately documented.

Based on the Data Breach Information Sheet and other relevant information, the Data Protection Officer should, in consultation with the Section Head involved in the breach, consider whether improvement measures (including administrative, procedural and/or technical measures, etc.) should be taken to reduce the likelihood of recurrence of similar breaches in the future. Possible improvement measures may include:

- The enhancement of security in handling personal data;
- The revision in the control of access rights of personal data granted to staff/data processors;
- The enhancement of IT security measures to protect personal data from hacking, unauthorised or accidental access, processing, erasure, loss or use;
- The revision of existing privacy policies and practices and/or the promulgation of new privacy policies and practices in light of the data breach with notification made to staff in writing;
- The enhancement of the effectiveness of detecting data breach – the keeping of proper logs and trails of access to personal data and ongoing monitoring of these logs and trails to detect unusual activities may provide early warning signs of unauthorised access to personal data;
- The strengthening of monitoring and supervision mechanism of staff and data processors;
  The additional provision of on-the-job training and circulation of information to promote privacy awareness and enhance prudence, competence and integrity of the staff who are responsible for handling personal data; and
- The revision of appointment policy of data processors and the review of the contractual terms with a data processor on protection of personal data privacy.

The Data Protection Officer should document the improvement measures by completing the "Post incident review" section of the Data Breach Information Sheet. After completing the Data Breach Information Sheet and no further clarification or information from the relevant Section is required, the Data Protection Officer can finalise the Information Sheet and submit to Chief Executive and Secretary for information. The Information Sheet can be filed afterwards.

The Data Protection Officer should also follow up on the implementation status of the improvement measures and consider selecting the Section encountering a data breach incident to participate in the periodic risk assessment.

For further details of data breach handling, please refer to the "Guidance on Data Breach Handling and the Giving of Breach Notifications" issued by the Privacy Commissioner[15].

[15] The Guidance Note can be found at
https://www.pcpd.org.hk//english/resources_centre/publications/files/DataBreachHandling2015_e.pdf

A-2f. Data Processor Management

Data processor is defined as "a person who (i) processes personal data on behalf of another person; and (ii) does not process the data for any of the person's own purposes" [16]. Tasks performed by data processors engaged by the HKIE include, but not limited to, the following –

- to carry out survey;
- to input personal data into computer systems;
- to scan documents which contain personal data; or
- to shred confidential documents which contain personal data.

Obligations of the HKIE as a data user under the PDPO

A data user is liable as the principal for the wrongful act of its authorised data processor[17]. According to the PDPO, if the HKIE engages a data processor, whether within or outside Hong Kong, to process personal data on behalf of the HKIE, the HKIE **must adopt** contractual or other means to prevent (i) any personal data transferred to the data processor from being kept longer than is necessary for processing of the data[18] and (ii) unauthorised or accidental access, processing, erasure, loss or use of the data transferred to the data processor for processing[19]. The Section Head that engages a data processor should ensure the adoption of appropriate means to manage the data processor as described below and may consult the Data Protection Officer for advice if required.

Management of data processor

Through contractual means
The subject officer engaging a data processor should incorporate the following terms on personal data protection in the service contract with the data processor where practicable and appropriate:

(a) The HKIE has the right to audit and inspect how the data processor handles and stores personal data;

(b) The data processor shall report immediately to the HKIE any loss of documents, security breaches or signs of abnormalities (e.g. if audit trail shows that a staff unusually accessed the personal data entrusted to the data processor);

(c) The data processor shall not use or disclose any personal data it receives or gains knowledge of for a purpose other than the purposes for which the personal data is entrusted to it by the HKIE;

(d) The data processor shall not sub-contract the service without the HKIE's approval;

(e) If the HKIE approves to sub-contract the services by the data processor, the data processor's contract with the sub-contractor should impose the same obligations in relation to data processing as those imposed on the data processor by the HKIE. If the sub-contractor fails to fulfil its obligations, the data processor shall remain fully liable to the HKIE for the fulfilment of its obligations;

[16] DPP2(4) in Schedule 1 to the PDPO.
[17] Section 65(2) of the PDPO.
[18] DPP2(3) in Schedule 1 to the PDPO.
[19] DPP 4(2) in Schedule 1 to the PDPO.

(f) The data processor shall ensure that it has personal data protection policies and procedures effectively in place and it provides adequate training to its relevant staff;

(g) The data processor shall ensure that appropriate security measures[20] are in place and the operations of the data processor are in full compliance with the PDPO including the DPPs. The data processor shall be required to adopt the same security measures that the HKIE has implemented in processing the data on its own; and

(h) Upon termination of the contract or when the personal data is no longer required for the purpose for which it is entrusted by the HKIE to the data processor, the data processor shall immediately return, destruct or delete the personal data.

For cross-border transfer arrangement, subject officer should consider incorporating the following terms on personal data protection in the service contract[21] with the transferee where practicable and appropriate:

(a) The transferee shall process or use the personal data for the purpose(s) as set out in this agreement to the exclusion of any other purpose;

(b) The transferee shall hold the personal data securely in accordance with the requirements of DPP4 of the PDPO. It will have in place appropriate technical and organisational measures and standards to protect the personal data against unauthorised or accidental access, processing, erasure, loss or use;

(c) The transferee shall not retain the personal data longer than is necessary for the fulfilment of the purpose(s) (including any directly related purpose(s)) for which the personal data is to be used;

(d) The transferee shall use the personal data exclusively for the purposes set out in this agreement and shall not transfer or disclose, either free of charge or in return for any benefits, the personal data to any other person, except when it is compelled to do so under the applicable laws;

(e) The transferee shall immediately rectify, erase or return the personal data on receiving instructions to this effect from the HKIE. The transferee undertakes in particular to rectify, erase or return all or part of the personal data if it appears that such measures are required by the requirements of the PDPO;

(f) The transferee has and shall at all times have in place accessible documents which clearly specify its policies and practices in relation to personal data;

(g) The transferee shall ensure that data subjects have rights of access to and correction of their personal data in the same way as they would have had under the PDPO; and

[20] The security measures that are appropriate and necessary will depend on the circumstances. Basically, the data processor should be required to take the same security measures that the HKIE would have taken if the HKIE was processing the data on its own.

[21] Sample contractual clauses for cross-border arrangement can be found at https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_crossborder_e.pdf

(h) Upon the HKIE's request, the transferee shall submit its data processing facilities, policies and procedures, data files, documentation and any other relevant information for reviewing, auditing and/or certifying by the HKIE or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the HKIE, to ascertain compliance with its warranties and undertakings in this agreement.

The above list is not exhaustive and the subject officer may need to change or add contractual obligations on the data processors based on different circumstances. Some key consideration factors include the amount of personal data to be entrusted to the data processor, the sensitivity of such personal data, the nature of the service to be provided and the harm that may result from a security breach.

For the terms on personal data protection in the service contract with the data processor, the respective Section may refer to templates at Annex E for reference.

Through other means

Apart from contractual means, the subject officer may also consider other means to manage the data processors engaged. Recommended measures include but not limited to:

- Performing a background check before engaging a data processor to ensure that it is (i) offering sufficient guarantees in respect of the technical competence and organisational measures governing the handling of personal data; and (ii) with a good track record on data protection; and

- Auditing and inspecting how the data processors handle and store personal data.

Review of the HKIE's management of data processors

If a Section engages a data processor, whether within or outside Hong Kong, to process personal data on behalf of the HKIE, Section Coordinator should perform a review of the data processors management **annually** by completing a Data Processor Review Checklist (please refer to Annex E of this PMP Manual for the checklist). The Section Coordinator should submit the completed checklist to the Data Protection Officer for his/her review.

A-2g. Communication

The HKIE is taking all practicable steps to communicate its personal data policies and practices to the general public and staff.

Communication to the Public

The Privacy Policy Statement is available for public access at the HKIE's website which informs the public of -

(i) the purpose and manner of the HKIE collecting personal data, including that, on or before the collection of personal data, the HKIE will provide a PICS to the data subject; and

(ii) their right to lodge a data access request or a data correction request, and the channel of lodging such requests, etc.

Any enquiries relating to personal data protection can be addressed to the Personal Data Privacy Officer.

Communication with the HKIE

The Data Protection Officer circulates this PMP Manual and other prevailing data privacy policies and guidelines to staff on **a half-yearly basis**, and keeps staff updated on any amendment to the Manual and the policies and guidelines.

Part B – Ongoing Assessment and Revision

Assessment and revision of personal data policies and practices should be carried out annually to ensure effectiveness of the PMP. The assessment and revision involve two parts – (1) Prepare an oversight and review plan and (2) review of the effectiveness of the PMP.

1. Prepare an Oversight and Review Plan

Review of the effectiveness of the PMP should be carried out in an annual cycle. Before the beginning of an annual cycle, the Data Protection Officer should prepare an oversight and review plan to set out how and when the review of the PMP should be carried out in the following year, as well as how the effectiveness of PMP will be monitored and assessed.

A suggested oversight and review plan covering the activities to be carried out by the Data Protection Officer in an annual cycle is provided below for reference.

Month 0 – Prepare and finalise the annual oversight and review plan

The Data Protection Officer should make reference to the suggested oversight and review plan and make necessary adjustments before the start of an annual cycle, for example, if the Data Protection Officer anticipates that Sections will need more than two months to update the personal data inventory, the Data Protection Officer may allow more time for this task.

Months 1 to 2 –

The tasks below can be carried out simultaneously:

(a) Carry out the Personal Data Inventory Review Exercise
The Data Protection Officer should initiate the Personal Data Inventory Review Exercise according to the Personal Data Inventory management guidelines (for details of the steps to be taken, please refer to Section 3 – Part A – 2a of this PMP Manual).

(b) Carry out the Review of the HKIE's management of data processors
The Data Protection Officer should initiate the Review of the HKIE's management of data processors according to the data processor management guidelines (for details of data processor management, please refer to Section 3 – Part A – 2f of this PMP Manual).

Months 3 to 4 – Carry out periodic risk assessments

The Data Protection Officer should initiate periodic risk assessments according to the risk assessments guidelines (for details of the steps to be taken, please refer to Section 3 – Part A – 2c of this PMP Manual).

Months 5 to 6 – Assess the effectiveness of the PMP Programme Controls

The Data Protection Officer should assess the effectiveness of the PMP with reference made to the ongoing assessment and revised policies/guidelines in relation to personal data by the PCPD (for details of the review checklist, please refer to Section 3 – Part B – 2 of this PMP Manual). If the Data Protection Officer finds any gaps in the implementation of the PMP, appropriate follow up actions should be taken in the following months, i.e. Months 7 to 8.

Months 7 to 10 – Review and revise this PMP Manual

The Data Protection Officer should review this PMP Manual and consider if any revision is needed. For instance, the Data Protection Officer should consider the following factors in evaluating whether revision is needed:

(a) Whether there are any new/revised regulatory requirements relating to personal data that may require corresponding changes to this PMP Manual;

(b) Whether there are any new/revised internal guidelines relating to personal data that may require corresponding changes to this PMP Manual;

(c) Whether there is any change within the HKIE that may require corresponding changes to this PMP Manual;

(d) Whether there are difficulties for the Sections in implementing the existing PMP Manual; and

(e) Whether the existing requirements under this PMP Manual need to be strengthened to enhance protection provided to data subjects, etc.

The Data Protection Officer should consult Chief Executive and Secretary and the Section Coordinators if any material change is to be made to the content of this PMP Manual.

Month 11 – Circulate this PMP Manual and other data privacy policies and guidelines

The Data Protection Officer should circulate the latest version of this PMP Manual and other data privacy policies and guidelines to all staff in the HKIE. The updated statement, if any, on personal information collection should also be made available for public access.

Month 12/Month 0 of the next yearly cycle – Review the execution of the oversight and review plan and prepare the plan for the next yearly cycle

The Data Protection Officer should complete the table in Section 3 – Part B – 2 to document the review results and report to Chief Executive and Secretary the execution of the oversight and review plan by the end of an annual cycle.

2. Review of PMP's Effectiveness

In order to document the annual review on the effectiveness of the PMP, the Data Protection Officer should complete the following review table and confirm that the actions set out under the oversight and review plan have been carried out appropriately.

Action	Completed/Not completed	Date of last review/update	Difficulties observed and proposed mitigation measures
1) Update of personal data inventory			
2) Periodic risk assessments			
3) Review and revise policies			
4) Training and education materials re-circulation and update (including risk mitigation measures drawn up from periodic risk assessments, case sharing regarding complaints and data breach incidents)			
5) Review of breach and incident management response protocols			
6) Data processor review			
7) Updates on the PMP have been communicated to staff			

Annex A – Guidelines on the Preparation of Personal Information Collection Statement ("PICS")

When the HKIE collects personal data from an individual, all practical steps should be taken on or before the collection to ensure that –

(i) the individual (i.e. the data subject) is informed of whether it is obligatory or voluntary for him/her to supply the personal data; and where it is obligatory for the data subject to supply his/her personal data, the consequences for the data subject if he/she does not do so; and

(ii) the data subject is explicitly informed of the purpose for which his/her personal data is to be used, the classes of persons to whom the data may be transferred or disclosed, the rights of the data subject to request access to and correction of the data, and the contact of the Personal Data Privacy Officer to whom any such request may be made.

In general, specific PICS should be used for specific collection purposes. A PICS should include the following information:

(a) **Statement of purpose:** This is a statement of the purpose for which the collected personal data will be used.

(b) **Statement as to whether it is obligatory or voluntary for the individual to supply his/her personal data:** On or before collecting any personal data from a data subject, the HKIE, as the data user, should inform the individual whether it is obligatory or voluntary for him/her to supply his/her personal data; the HKIE should also inform the individual of the consequences if failing to supply his/her personal data.

(c) **Statement of possible transferees:** This statement should declare the classes of persons to whom personal data collected from the data subjects may be transferred or disclosed, for instance, data processor engaged to process personal data held by the HKIE.

(d) **Statement of rights of access and correction:** This statement should inform the data subject that he/she has the right to request access to and correction of his/her personal data that is held by the HKIE.

(e) **Contact person for requesting access or correction:** The data subject should be informed of the post title and contact details of the staff member who is responsible for handling data access and data correction requests.

Template of Personal Information Collection Statement for Event

Any personal data provided in this registration form will be used for the purposes directly related to the processing of your registration and carrying out activities related to this event. You are required to supply the data in order to register for this event. The personal data provided may be transferred to other parties for purposes relating to this event where necessary. The HKIE intends to use the personal data you provided for the purpose of sending you information on other HKIE's activities. You may request access to or correction of your personal data by addressing your request to the Event Secretariat.

(Include these lines as appropriate)

Developing a PICS

When developing a PICS, reference can be made to the samples below.

Example of a General PICS

[COMPANY/ORGANISATION] may collect your personal data to handle your [enquiries/complaints]. The provision of your personal data is voluntary. If you do not provide sufficient information, [COMPANY/ORGANISATION] may not be able to process your [enquiries/complaints]. [COMPANY/ORGANISATION] may transfer your personal data to a [third party sub-contractor] to handle your [enquiries/complaints] ***OR*** *will not transfer your personal data to third party.] Please also note that the aforementioned third parties may or may not be located within Hong Kong, and your information may be subject to cross-border transfer to places outside Hong Kong for necessary handling or processing.*

You have the right to request access to and correction of your personal data held by [COMPANY/ORGANISATION]·

Such request should be made in writing to the Data Protection Officer at the address: [to be inserted with [COMPANY's/ORGANISATION's] address]. For details of privacy policy, you may refer to [COMPANY's/ORGANISATION's] Privacy Policy Statement at [*to be inserted with [COMPANY's/ORGANISATION's] website].*

Note: Information in < > should be replaced with the relevant purpose and third parties involved, if any.

The following samples of PICSs are developed for several common scenarios where personal data may be collected from members of the public, i.e., recruitment and handling of complaints.

Example 1: Employment – related records

[COMPANY/ORGANISATION]

Personal Information Collection Statement for Recruitment

The personal data provided in the application forms for openings in [COMPANY/ORGANISATION] will be used for recruitment and other employment-related purposes. It may be provided to its subsidiaries and other organisations or agencies authorised by [COMPANY/ORGANISATION] to process the information for purposes relating to recruitment by and employment with [COMPANY/ORGANISATION] e.g. qualifications assessment, medical examination, employer reference and integrity checking, etc. where necessary.	→ Purpose Statement → Classes of transferees
Your provision of the personal data requested in the application forms is obligatory, except for the items marked as optional. Your application will not be considered if you fail to provide all of the required information or it is not clear from your statements that you have the minimum qualifications, training, experience or other requirements specified for the job. You are requested to notify [COMPANY/ORGANISATION] if there are any subsequent changes to the information provided after submission of the application form.	→Obligatory to provide data →Consequences if failing to supply his/her personal data (for obligatory)
Information on unsuccessful candidates will normally be destroyed 24 months after rejection of the candidate's application.	→ Statement of retention period
You have the right to request access to and correction of your personal data held by [COMPANY/ORGANISATION]. Such request should be made in writing to the Data Protection Officer at the address: [to be inserted with [COMPANY's/ORGANISATION's] address. For details of [COMPANY's/ORGANISATION's] privacy policy, you may refer to [COMPANY's/ORGANISATION's] Privacy Policy Statement at [to be inserted with [COMPANY's/ORGANISATION's] website.	→Access and correction right →Contact person

Example 2: General Administrative records

[COMPANY/ORGANISATION]

Personal Information Collection Statement
for handling complaints

All personal data provided will be used for purposes directly related to the handling of this complaint. The personal data provided may be transferred to other parties with whom is necessary during the handling of this complaint, including the party being complained against or other parties concerned, where necessary.	→ Purpose Statement → Classes of transferees
It is voluntary for you to supply your personal data to [COMPANY/ORGANISATION]. Information on your complaint will normally be destroyed xx months after the handling and follow up of your complaint is completed.	→ Optional to provide data → Statement of retention period
You have the right to request access to and correction of your personal data held by [COMPANY/ORGANISATION]. Such request should be made in writing to the Data Protection Officer of [COMPANY/ORGANISATION] at the address: [to be inserted with [COMPANY's/ORGANISATION's] address. For details of [COMPANY's/ORGANISATION's] privacy policy, you may refer to [COMPANY's/ORGANISATION's] Privacy Policy Statement at [to be inserted with *[COMPANY's/ORGANISATION's]* website.	→Access and correction right →Contact person

Example 3: Competition enrollment - related records

[COMPANY/ORGANISATION]

Personal Information Collection Statement
for handling complaints

The personal data provided in the enrolment form for this Poster Design Competition organised by [COMPANY/ORGANISATION] will be used for this competition and other relevant subsequent follow-up actions only. The personal data may be transferred to other parties for purposes relating to this competition and subsequent follow-up actions, where necessary.	→ Purpose Statement → Classes of transferees
Items (a), (b), (c), (d) and (e) are mandatory for [COMPANY/ORGANISATION] to verify your eligibility to enter into this competition. Your enrollment will not be considered if you fail to provide these information. *Item (f), (g) and (h) are voluntary. Your chance of entering into this competition will not be affected if you do not provide these information.* *Your personal data will normally be destroyed 1 year after the competition is completed.*	→ Optional to provide data → Consequences if failing to supply his/her personal data (for obligatory) → Optional to provide data → Statement of retention period
You have the right to request access to and correction of your personal data held by [COMPANY/ORGANISATION]. Such request should be made in writing to the Data Protection Officer at the address: [to be inserted with [COMPANY's/ORGANISATION's] address. For details of [COMPANY's/ORGANISATION's] privacy policy, you may refer to [COMPANY's/ORGANISATION's] Privacy Policy Statement at [to be inserted with *[COMPANY's/ORGANISATION's]* website.	→Access and correction right →Contact person

For further details relating to preparation of PICS, please refer to the "Guidance on Preparing Personal Information Collection Statement and Privacy Policy statement"[22] issued by the Privacy Commissioner.

[22] The Guidance Note can be found at https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_picspps_e.pdf

A. Checklist for the Preparation of PICS

When it is required to develop a PICS, the respective Section should prepare it based on the checklist in the following page. The purpose of the checklist is to ensure that (i) the required and optional information is stated in the PICS, and (ii) the presentation of the PICS is appropriate. The draft PICS prepared by the respective Section should be submitted to the Data Protection Officer for approval.

Checklist for the Preparation of PICS

Part 1: Required Information – Must include the following items when preparing a PICS

	Item	Checked ☑
1.	The PICS should inform the data subject of the following information:	□
(a)	a statement of the purpose for which the personal data collected will be used	□
(bi)	a statement of whether it is obligatory or voluntary for the data subject to supply his/her personal data	□
(bii)	a statement of the consequences if he/she fail to supply his/her personal data where it is obligatory to do so	□
(c)	a statement of the classes of persons to whom personal data collected may be transferred or disclosed	□
(d)	a statement of the data subject's rights to request access to and correction of his/her personal data	□
(e)	the contact for data subject to request for access or correction of their personal data	□
	If applicable	
(f)	a statement of the retention period	□

Part 2: Presentation of PICS

	Item	Checked ☑
2.	The PICS will be provided to the data subject on or before collecting his/her personal data.	□
3.	The purpose statement is not too vague or too wide in scope.	□
4.	User-friendly language (e.g. the choice of simple rather than difficult words and the avoidance of use of legal terms or convoluted phrases) and presentation are used.	□
5.	The layout and presentation of the PICS (including the font size, spacing, underlining, use of headings, highlights and contrasts) has been designed so that the PICS is easily readable to individuals with normal eyesight.	□
6.	The PICS is presented in a conspicuous manner (e.g. the PICS is a stand-alone section and its contents are not buried among other information).	□

Reference:

"Guidance on Preparing Personal Information Collection Statement and Privacy Policy Statement" issued by the office of the Privacy Commissioner for Personal Data, Hong Kong at https://www.pcpd.org.hk//english/resources_centre/publications/files/GN_picspps_e.pdf.

Annex B – Data Access and Correction Policy

This document details the HKIE's policy in handling data access requests ("DARs") and data correction requests ("DCRs").

Background

According to Data Protection Principle 6 of the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO"), an individual has the right to (i) request access to his/her own personal data held by a data user, and (ii) request the correction of personal data if it is inaccurate. The individual, or his/her relevant person[22], may submit a DAR under section 18(1) of the PDPO to request a data user to (i) inform him/her whether the data user holds the individual's personal data; and (ii) if the data user holds such data, supply the individual with a copy of such data.

If the individual considers the personal data supplied by a data user pursuant to a DAR is inaccurate, a DCR can be made to request the data user to correct his/her personal data under section 22(1) of the PDPO.

Handling DARs

Receipt of DARs

An individual may make a DAR to the respective Section of the HKIE by email or by post.

Handling DARs

According to section 19(1)(a) of the PDPO, the HKIE must respond within **40 calendar days** after receiving a DAR. Upon receipt of a DAR, the respective Section should take the following steps as soon as practicable, and the whole process should not take more than 40 calendar days unless it is necessary.

If the HKIE is unable to comply with a DAR within 40 calendar days (e.g. the requested data is voluminous or if the DAR fee[23] is received close to the expiry of the 40 days so that more time is required for the data user to comply with the DAR), the respective Section should give the requestor a written notification of the situation with reasons within the 40 day period and comply with the DAR to the extent that the HKIE is able to[24]. The HKIE is required to comply fully with the DAR as soon as practicable thereafter[25].

---

[22] "Relevant person" is defined under section 17A of the PDPO as a person authorised in writing by the individual to make a data access or correction request on his/her behalf. In addition, according to section 2 of the PDPO, "relevant person" means a person (1) who has parental responsibility for the minor individual; (2) who has been appointed by a court to manage affairs related to an individual that is incapable of managing his own affairs; or (3) who has been appointed to be the guardian of an individual that is mentally incapacitated (please refer to section 2 of the Mental Health Ordinance (Cap 136)).

[23] See *Step 4 – Ascertain whether payment would be charged on the DAR* of this Annex.

[24] Section 19(2)(a) of the PDPO.

[25] Section 19(2)(b) of the PDPO.

Recording DARs

The respective Section should keep a register of all DARs received.

Step 1 – Verify the identity of the requestor

The respective Section should ascertain the identity of the requestor upon receipt of a DAR.

If the requestor is requesting his/her own personal data, the respective Section should require the requestor to provide his/her proof of identity (e.g. name and application/membership number).

If the DAR is made by a relevant person on behalf of an individual, the respective Section should require the requestor to provide the proof of identity of the individual (e.g. relationship between the requestor and individual concerned; name, date of birth and application/membership number of the individual.

If required, part of the HKID Card number (e.g. the first or last few characters) of the individual to whom the requested personal data belongs to should be obtained from the requestor.

Written request from individual is needed if the individual asks the HKIE to provide his/her personal information in written form.

A written authorisation signed by the individual to whom the requested personal data belongs to has to be provided by the relevant person if the requested information will be provided by the HKIE in writing.

If an individual is incapable of managing his/her own affairs, the requestor should provide evidence to prove such claim.

After verifying the identity of the individual to whom the requested personal data belongs to, the respective Section may proceed to Step 2.

If the identity of the individual cannot be verified, the respective Section may refer to the **"Steps to Take in Refusing to Comply with a DAR"** section below and refuse to comply with the DAR in accordance with Section 20(1)(a) of the PDPO.

Step 2 – Verify whether the HKIE holds the requested information

The respective Section should locate the requested personal data within the HKIE, and pass on the request to other Sections if the requested data is held by them.

If the respective Section successfully locates the requested data, the respective Section should proceed to Step 3.

If the respective Section confirms that the HKIE does not hold the requested data, the respective Section should inform the requestor in writing that the HKIE does not hold the requested data **within 40 calendar days** in accordance with section 19(1)(b) of the PDPO.

If the respective Section requires further information to locate/check the availability of the requested data, the respective Section should obtain further information from the requestor. If no further information is provided by the requestor, the respective Section may refer to the **"Steps to Take in Refusing to Comply with a DAR"** section below and refuse to comply with the DAR in accordance with section 20(3)(b) of the PDPO.

Step 3 – Ascertain whether the requested information located contains personal data of any third party

The respective Section should review the requested information located in Step 2 and ascertain whether such information contains personal data of other individuals.

If the information does not contain personal data of any third party, the Personal Data Privacy Officer may proceed to Step 4.

If the information contains personal data of a third party, before proceeding to Step 4, the respective Section should either –

(i) obtain the third party's consent for the release of his/her personal data to the requestor of the DAR; or
(ii) redact the third party's personal data from the copy of the information to be provided to the requestor.

Step 4 – Ascertain whether payment would be charged on the DAR

A data user may (i) impose a fee for complying with a DAR[26] and (ii) refuse to comply with a DAR unless and until any fee imposed has been paid[27]. No fee imposed shall be excessive (i.e. exceeding the costs of complying with the DAR).

The costs of complying with a DAR may vary with the scope and complexity of the request and the respective Section may consider the following items when calculating the fee:

- Direct labour costs and necessary expenses – A data user may take into account the direct costs attributable to the time spent by its staff and the actual out-of-pocket expenses for locating, retrieving and reproducing the requested data for complying with the DAR. Such costs may include the labour cost attributable to the time spent on extracting or editing the requested data, provided that such tasks are directly related to and necessary for compliance with the DAR.
- Photocopying
- Flat-rate fee – the HKIE may impose a flat-rate fee if the requested data is kept in a digital format and the HKIE would operate standard procedures to retrieve such records. Charging a flat-rate fee is permissible, provided that the fee imposed is lower than the direct and necessary costs for complying with a DAR and in any event not excessive under normal circumstances.

The respective Section should determine whether, and if so, how much would be charged in accordance with section 28 of the PDPO and proceed to Step 5.

Step 5 – Provide the requested information to the requestor

If payment is required, the respective Section should inform the requestor of the amount of payment to be charged and make arrangements for the payment. When the requestor agrees the payment, the Finance Section of the HKIE may issue a demand note to the requestor as appropriate. The respective Section should pass a copy of the personal data to the requestor within 40 calendar days after the DAR is received from the requestor. -

If no payment is received from the requestor, the respective Section may refer to the **"Steps to Take in Refusing to Comply with a DAR"** section below and notify the requestor of the HKIE's refusal to comply with the DAR in accordance with section 28(5) of the PDPO.

If payment is not required, the respective Section should provide a copy of the requested personal data to the requestor.

Refuse to comply with a DAR

The respective Section should not reject a DAR unless under the circumstances specified in the PDPO.

Whereas the above-mentioned steps of handling DARs have only listed a few circumstances where the respective Section may refuse a DAR, a **full list of the circumstances** provided for in the PDPO is specified below.

[26] Section 28(2) of the PDPO.
[27] Section 28(5) of the PDPO.

According to section 20(1) of the PDPO, the HKIE shall refuse to comply with a DAR if:

(a) the HKIE is not supplied with information reasonably required to satisfy as to the identity of the requestor;
(b) the HKIE cannot comply with the request without disclosing the personal data of a third party (subject to redaction of third party's personal data, see Step 3 above); or
(c) where compliance with the request is for the time being prohibited under the PDPO or any other ordinance.

In addition, the PDPO provides under section 20(3) the following grounds upon which the HKIE as a data user may rely on to refuse to comply with a DAR:

(a) the request if not in writing, in Chinese or English;
(b) the HKIE is not supplied with information to locate the requested data;
(c) the request follows two or more similar requests, and it is unreasonable for the HKIE to comply with the request in the circumstances;
(d) another party controls the use of the requested data in a way that prohibits the HKIE from complying with the request; or
(e) the HKIE is entitled under the PDPO or any other ordinance not to comply with the request; or there is an applicable exemption provided for in the PDPO from the requirement to comply with the request.

Also, under section 28(5) of the PDPO, the HKIE may refuse to comply with a DAR unless and until any fee imposed for complying with the request has been paid.

Steps to Take in Refusing to Comply with a DAR

When the HKIE rejects a DAR, the respective Section should carry out the following procedures for refusing to comply with a request:

1. The respective Section should give **written notice** and reasons for refusal to the requestor **within 40 calendar days** from receiving the request[28];
2. Where there is another data user that controls the use of the data in such a way that prohibits the HKIE from complying with the request, the respective Section should inform the requestor of the name and address of the other data user concerned in the notification of refusal[29]; and
3. The respective Section is also required to keep a log entry containing the particulars of the reasons for the refusal of the request for four years[30].

[28] Section 21 (1)(a) of the PDPO.
[29] Section 21 (1)(c) of the PDPO.
[30] Section 27 of the PDPO.

Handling DCRs

Receipt of DCRs

After complying with a DAR, the HKIE should assess whether any subsequent correspondence from the requestor would constitute a DCR. If a requestor replies to the HKIE and points out any inaccuracy in the copy of his/her personal data and requests correction of such data, the correspondence would generally constitute a DCR even if the requestor does not make reference to any provisions under the PDPO in relation to DCR.

Recording DCRs

The respective Section should keep a register for all DCRs received.

Handling DCRs

According to section 23(1) of the PDPO, the HKIE must respond within **40 calendar days** after receiving a DCR. Upon receipt of a DCR, the respective Section should take the steps stipulated below as soon as practicable, and the whole process should not take more than 40 calendar days unless it is necessary.

If the HKIE is unable to comply with a DCR within 40 days (e.g. the data to be corrected is voluminous), the HKIE should give the requestor a written notification of the situation with reason(s) within the 40-day period, and comply with the DCR to the extent that the HKIE is able to [31]. The HKIE is required to comply with the DCR as soon as practicable thereafter[32].

Step 1 – Verify the identity of the requestor

The respective Section should ascertain the identity of the requestor. If the DCR is preceded by a DAR, the respective Section may make reference to the identity proof provided by the requestor for his/her DAR.

If the requestor is requesting for a DCR for his/her own personal data, the respective Section should require the requestor to provide his/her proof of identity (e.g. name and application/membership number).

If the DCR is made by a relevant person on behalf of an individual, the respective Section should require the requestor to provide the proof of identity of the individual (e.g. relationship between the requestor and individual concerned; name of the requestor; name, date of birth and application/membership number of the individual).

If required, part of the HKID Card number (e.g. the first or last few characters) of the individual to whom the personal data belongs to can be obtained from the requestor.

After verifying the identity of the individual to whom the requested personal data belongs to, the respective Section may proceed to Step 2.

If the identity of the individual or the relevant person cannot be verified, the respective Section may refer to the "**Steps to Take in Refusing to Comply with a DCR**" section below and refuse to comply with the DCR in accordance with section 24(1) of the PDPO.

---

[31] Section 23(2)(a) of the PDPO.
[32] Section 23(2)(b) of the PDPO.

Step 2 – Assess whether the personal data to which a DCR relates is inaccurate

Before complying with or refusing to comply with a DCR, relevant officers handling the DCR should **not** disclose to a third party the personal data to which the DCR relates. In case the relevant officers have reason to do so, the officer should take all practicable steps to advise the third party concerned that the data is being considered for correction[33].

The respective Section should consider whether the personal data in question is inaccurate. If the respective Section confirms that the data is inaccurate, the HKIE should comply with the DCR and the respective Section should proceed to Step 3.

If the personal data to which the DCR relates was provided by a third party instead of collected from the individual directly, the respective Section may consult the third party for the accuracy of such data.

If the respective Section (1) is **not** satisfied that the personal data to which the DCR relates is inaccurate or the correction provided in the DCR is accurate, or (2) considers that the data to which a DCR relates is an expression of opinion[34] and the respective Section is **not** satisfied that the opinion is inaccurate, the respective Section may refer to the "**Steps to Take in Refusing to Comply with a DCR**" section below and inform the requestor of the reasons for refusal in accordance with section 24(3)(b) or (d) or section 25(2) of the PDPO.

Step 3 – Correct the data

If the respective Section considers that the data is inaccurate, the Section should make the necessary correction and confirmation should be sent to the individual to whom the personal data belongs to after completion of the DCR within 40 calendar days after receiving the DCR.

The HKIE is **not** entitled to impose a fee for complying with a DCR[35].

If the inaccurate data has been disclosed to a third party during the past 12 months before the date of correction of the data in compliance with a DCR, the respective Section should ascertain whether the third party has ceased using that data. And if possible, the respective Section should take all practicable steps to supply such third party with a copy of the corrected personal data and a written notice of the reasons for the correction[36], except where the third party has been supplied a copy certified correct by the data user.

Refuse to comply with a DCR

The respective Section should not reject a DCR unless under the circumstances specified in the PDPO.

Whereas the above-mentioned steps of handling DCRs only list a few circumstances where the respective Section may refuse a DCR, a full list of the circumstances provided for in the PDPO is specified as below.

---

[33] Section 22(3) of the PDPO.
[34] For example, statements made by an appraising officer in a performance appraisal report about the performance of the appraisee may consist of mostly expressions of opinion and partly fact. While comments on the appraisee's competencies are generally expression of opinion, statements on which duties have been performed by the appraisee during the appraisal period are likely questions of fact.
[35] Section 28(1) of the PDPO.
[36] Section 23(1)(c) of the PDPO.

According to section 24 of the PDPO, the HKIE may refuse to comply with a DCR if:

(a) the request is not in writing, in Chinese or English;
(b) the HKIE is not satisfied that the personal data to which the DCR relates to is inaccurate;
(c) the requestor does not provide sufficient information for the HKIE to ascertain in what way the data is inaccurate;
(d) the HKIE is not satisfied that the correction requested is accurate;
(e) the respective Section is not supplied with the reasonably required information to ascertain the identity of the requestor or establish the relationship between the relevant person and the data subject; or
(f) there is another data user that controls the processing of the data in such a way as to prohibit the HKIE from complying with the DCR.

Steps to Take in Refusing to Comply with a DCR

When the HKIE rejects a DCR, the respective Section should carry out the following procedures for refusing to comply with a request:

1. The respective Section should give **written notice** and reasons for refusal to the requestor **within 40 calendar days** from receiving the request[37];
2. Where there is another data user that controls the use of the data in such a way that prohibits the HKIE from complying with the request, the respective Section should inform the requestor of the name and address of the other data user concerned in the notification of refusal to comply with the request to the requestor[38];
3. Where the personal data to which a DCR relates to is an expression of opinion and the respective Section is not satisfied that the opinion is inaccurate, he/she should make a note of the requestor's correction request. This should be annexed to the data concerned in such a way that it is drawn to the attention of, or made available for inspection by, any person (including the HKIE or a third party) who may use such data in future[39]. The respective Section should also attach a copy of the note to the notice of refusal[40]; and
4. The respective Section is also required to keep a log entry containing the particulars of the reasons for the refusal of the request for four years[41].

For further details relating to data access request and data correction request handling, please refer to the "Proper Handling of Data Access Request and Charging of Data Access Request Fee by Data Users"[42] and the "Guidance on the Proper Handling of Data Correction Request by Data Users"[43] issued by the PCPD.

---

37 Section 25(1)(a) of the PDPO.
38 Section 24(3)(e) and Section 25(1)(b) of the PDPO.
39 Section 25(2) of the PDPO.
40 Section 25(2)(ii) of the PDPO.
41 Section 27 of the PDPO.
42 The Guidance Note can be found at https://www.pcpd.org.hk//english/resources_centre/publications/files/DAR_e.pdf.
43 The Guidance Notes can be found at https://www.pcpd.org.hk//english/resources_centre/publications/files/DCR_e.pdf.

Annex C – Personal Data Correction Request Form

(*In accordance with section 22(1) of the Personal Data (Privacy) Ordinance (Cap. 486), where a data subject* ***has been provided with a copy of his personal data after making a data access request*** *and he considers that the data are inaccurate, he may make a request that the data user make the necessary correction to the data).*

I. Requestor's Personal Particulars

Name (in full)	
Contact number	
Fax number or email address	
Hong Kong Identity Card Number (Note 1)	
Please state the personal data you are requesting to have corrected or updated (attach additional sheets if necessary)	
Please provide the corrected or updated personal data (attach additional sheets if necessary)	

II. Personal Particulars of the Data Subject (if different from that of the requestor)

Name (in full)	
Contact number	
Fax number or email address	
Hong Kong Identity Card Number (Note 1)	
Please state the personal data you are requesting to have corrected or updated (attach additional sheets if necessary)	
Please provide the corrected or updated personal data (attach additional sheets if necessary)	

III. Terms and conditions

I, _____ hereby declare and confirm that all information given in this form and all supporting documents in connection with this Correction Request are true, accurate and complete. I understand that it will be necessary for [COMPANY/ORGANISATION] to verify my identity and that [COMPANY/ORGANISATION] may contact me for more detailed information in order to correct or update the personal data requested and I consent to the collection, use and disclosure of the personal data that I have provided in this form for the purpose of complying with my correction request.

Signature: _____ Date: _____

Important Notes:

1. The Hong Kong Identity Card Number need not be provided in this Form if you have reasonable grounds to believe that this will not be necessary for the unique identification of the data subject in the circumstances. However, [COMPANY/ORGANISATION] may, under some circumstances, require you to supply such information as necessary to prove the identity of the data subject as permitted under the provisions of Personal Data (Privacy) Ordinance.

2. The information provided will be used for processing data correction requests. The provision of personal data is voluntary. However, if you do not provide sufficient information, we may not be able to process your request.

3. Please submit the completed form to any post office or send it to the Personal Data Privacy Officer of [COMPANY/ORGANISATION] by email (to be inserted with organisation's website) or by post to the following address –

> [*to be inserted with [COMPANY's/ORGANISATION's] contact details*]
> *Personal Data Privacy Officer*
> [*to be inserted with [COMPANY's/ORGANISATION's] address*]

4. If the request is made by an individual other than the data subject, an authorisation letter signed by the data subject and information that can provide proof of the identity of the data subject and further proof of the requestor's status as a relevant person should be enclosed.

5. If you have any queries / need any guidance in filling up this form, please contact us at email: [*to be inserted with [COMPANY's/ORGANISATION's] website*].

Annex D – Complaints and Enquiries Handling Policy

When complaints and enquiries regarding personal data privacy and practices and the HKIE compliance with the PDPO are received from the public in writing, the following procedures should be performed:

Step 1: Register the complaint or enquiry case into the complaint/enquiry register and notify the Personal Data Privacy Officer and Data Protection Officer

When a personal data privacy complaint or enquiry is received in writing, the respective Section should register the complaint in the complaint/enquiry register and notify the Personal Data Privacy Officer and Data Protection Officer.

Step 2: Conduct an investigation and draft a reply by the respective Section

Upon receiving the personal data privacy complaint or enquiry, the respective Section should conduct investigation of the case. If required, the respective Section may seek data privacy advices from the Personal Data Privacy Officer and Data Protection Officer. In addition, the respective Section should draft a reply to the complainant/enquirer and agree with the Personal Data Privacy Officer and Data Protection Officer on the draft reply.

Step 3: Report to the Personal Data Privacy Officer and Data Protection Officer for completion of the case

The respective Section should report the completion of the case to the Personal Data Privacy Officer and Data Protection Officer and he/she should record the close of the case into the complaint/enquiry register.

Note: If the HKIE's practice/policy/guidelines in relation to personal data handling are changed due to complaint case, the Personal Data Privacy Officer/Data Protection Officer should (i) share the case with staff as a training; (ii) assess whether an update of this PMP Manual is needed; and (iii) notify staff of the change of the practice/policy/guidelines in relation to personal data handling.

Template of Complaint and Enquiry Register

Date of receipt of the compliant/ enquiry in writing	Brief description of the complaint/ enquiry	Name of the complainant /enquirer	Notified Personal Data Privacy Officer and Data Protection Officer on (date)	Replied to the complainant/ enquirer on (date)	Reported to Personal Data Privacy Officer and Data Protection Officer on case completion on (date)	Handled by	
						Section	Staff Name

Annex E – Templates of the Terms on Personal Data Protection in the Service Contract with Data Processor

Undertaking by Data Processor on Data Protection

To preserve the confidentiality of all information that the [Organisation Name] provides to [Data Processor], [Data Processor] agrees and warrants that:-

1. all information provided by the [Organisation Name] will be treated as confidential.

2. all personal data provided by the [Organisation Name] are handled in accordance with the relevant provisions of the Personal Data (Privacy) Ordinance in Hong Kong.

3. [Data Processor] collects Personal Data from the [Organisation Name] only to the extent necessary for its service provision to the [Organisation Name], and never submits or discloses such data to any third party.

4. all information provided by the [Organisation Name] which contains personal data will be disposed properly upon completion of its service provision.

Signed for and on behalf of
[Data Processor]

By _____

Name:

Date:

(To be attached to and forming part of the Agreement(s) for provision of services by the Data Processors.)

ANNEX

This Annex is made on _____ (dd/mm/yy) between: -

(1) **(Name of the Contractor)** (hereinafter called "the Contractor") whose registered office is situated at _____ _____ of the one part, and

(2) **[Organisation Name]** (hereinafter called "XXXX") whose registered office is situated at 9/F Island Beverley, No 1 Great George Street, Causeway Bay, Hong Kong of the other part.

(individually a "Party" and collectively the "Parties")

THE PARTIES HEREBY AGREE AS FOLLOWS:

1. Definitions and Interpretation

Unless otherwise stated herein, the following words and expressions shall have the same meanings as used in this Annex:-

- "Agreement" means the Contract (as hereinafter defined) including this Annex being incorporated as part of the Contract.

- "Contract" means the contract, purchase order or confirmation mutually agreed and duly signed by the Contractor and the [Organisation Name] respectively for provision of [services] by the Contractor to the [Organisation Name] in respect of the Subject Materials (as hereinafter defined) as specified therein.

- "Members" means members of the HKIE.

- "Personal Data" means any data from which it is practicable for the identity of any individual to be directly or indirectly ascertained and in a form in which access to or processing of the data is practicable.

- "Subject Materials" means any or all of the following materials or items specified in the Contract and provided by the [Organisation Name] to the Contractor which contain Personal Data of the Members and other persons to which such Personal Data may be related, including without limitation their names, addresses and other particulars:
  (a) address labels or other kinds of labels or tags;
  (b) letters, forms, advice or notifications;
  (c) (Organisation Name)'s journals and other publications; or
  (d) other items or materials as may be specified in the Contract by the (Organisation Name) for the purposes of this Agreement.

2. Contractor's Undertakings

The Contractor hereby agrees with and undertakes to the [Organisation Name] as follows:

2.1 The Contractor shall collect the Subject Materials at the registered address of the [Organisation Name] for the purposes of this Agreement.

2.2 The Subject Materials shall be collected by authorised personnel of the Contractor only.

2.3 The authorised personnel of the Contractor shall acknowledge the collection of the Subject Materials from the [Organisation Name] by stamping its company chop.

2.4 Only transportation vehicles authorised by the Contractor shall be used for transportation of the Subject Materials to the Contractor's workshop.

2.5 The number of the Subject Materials collected shall be checked by authorised personnel of the Contractor at the Contractor's workshop against the collection forms verified by the [Organisation Name] to ensure the Subject Materials collected by the Contractor are in order.

2.6 The Contractor shall procure and ensure their personnel shall take appropriate measures to ensure the Subject Materials and the relevant Personal Data are handled and protected in such manner and at such security level appropriate to the harm, loss or damage that may result from any unauthorised or unlawful processing/use or accidental loss, destruction or damage of the same.

2.7 All Subject Materials and the relevant Personal Data shall remain confidential, and access to the Subject Materials shall be restricted to personnel designated and authorised by the Contractor during the whole service provision process.

2.8 The Contractor's personnel shall only use the Subject Materials for the purposes set out in this Agreement.

2.9 All the Subject Materials collected are treated in strict confidence and under no circumstance will any of the Personal Data in the Subject Materials be disclosed to a third party without the authority of the [Organisation Name].

2.10 The Contractor shall fully indemnify and hold the [Organisation Name] harmless from and against any and all claims, demands and actions and all damages, losses, costs and expenses arising in connection with any breach by the Contractor of the provisions of this Agreement and the Personal Data (Privacy) Ordinance relating thereto.

3. HKIE's Undertakings

3.1 The [Organisation Name] shall ensure that the Subject Materials are printed and packed properly, and are placed in a designated collection place ready for collection by authorised personnel of the Contractor in accordance with the agreed schedules.

3.2 The [Organisation Name] shall notify the Contractor of the number of each batch of Subject Materials for collection.

4. Warranties

4.1 The Contractor warrants that it will process the Personal Data in compliance with the Personal Data (Privacy) Ordinance, Chapter 486 of the Laws of The Hong Kong SAR, and in accordance with the terms and conditions in this Annex.

4.2 The Contractor warrants that in order to observe the rights of ownership of the [Organisation Name] in the Personal Data, it will not copy, retain or process the Personal Data in any manner over the course and after expiration or termination of this Agreement other than in accordance with the provisions of this Agreement.

5. Appointment of/Compliance by Sub-contractor

5.1 The Contractor may authorise a sub-contractor to process the Subject Materials for provision of services for the [Organisation Name] subject to the prior written consent by the [Organisation Name] which may from time to time be given or withdrawn by the HKIE at its discretion.

5.2 The Contractor shall provide full details and information of the sub-contractor and their personnel to the [Organisation Name] as the [Organisation Name] may from time to time request.

5.3 The Contractor shall procure and ensure that the sub-contractor shall fully observe and be bound by the same terms and conditions applicable to the Contractor as stated in this Annex as if the sub-contractor were party to this Annex in place of the Contractor, and the Contractor shall remain fully responsible and liable for the acts and defaults of the sub-contractor.

6. Miscellaneous

6.1 Except as provided herein, the Contractor's rights, interests or obligations in this Agreement may not be assigned, nor any duties delegated, without the prior written consent of the [Organisation Name].

6.2 The failure of any of the Parties to enforce any of the provisions of this Agreement or any rights with respect hereto shall in no way operate or be considered a waiver of such provision or right, or in any way affect the validity of this Agreement. The waiver of any breach of this Agreement by any Party shall not operate or be considered a waiver of any other prior or subsequent breach.

6.3 This Agreement shall be subject to and governed by the laws of The Hong Kong SAR.

For and on behalf of [NAME OF THE CONTRACTOR]	For and on behalf of [ORGANISATION NAME]
Authorised signature with company chop	Authorised signature with company chop
Full name in BLOCK letters	Full name in BLOCK letters
Title : _____	Title: _____
Date : _____	Date : _____
in the presence of (name of witness)	in the presence of (name of witness)
Signature of witness	Signature of witness
Date : _____	Date : _____

Undertaking by Contractor
of
the Service Contract
of
[Project Name] for
[ORGANISATION NAME]

Client: [Organisation Name]

Contractor:

Quotation and Sales Order Reference:

1. I (The Contractor) undertake to hold in strict confidence all information that I (the Contractor) have access to through my position as the contractor, its representative, employee, agent, associate, sub-contractor, consultant or any other persons engaged on any work in connection with the above service contract for providing [service] for the Client.

2. I (The Contractor) undertake not to make any unauthorised disclosure or take advantage of any information whether or not for personal gain.

3. I (The Contractor) understand that the Client may take actions against the Contractor in accordance with all pertinent laws, regulations and ordinances of the Hong Kong SAR as a result of any breach of confidence (whether under this service contract or general law) by any such persons.

4. I (The Contractor) understand that I (the Contractor) shall comply with the requirements of the above service contract and the IT Security Policy, if any, of the Client.

Signed and Chopped _____

Name (block letter) _____

Date _____

Confidentiality of Information

The Contractor shall ensure that the Relevant Employees comply with the following provisions on the Confidentiality of Information.

1. The Contractor shall treat as confidential all information, drawings, specifications, documents, contracts, design materials and all other data (including without limitation any personal particulars records and Personal Data (as defined in the Personal Data (Privacy) Ordinance (Cap 486)) and materials of any nature (in or on whatever media) which the Client has for the purposes of or in the course of performing this Service Contract supplied, made available or communicated to the Contractor or are otherwise accessible by the Contractor and which the Client has designated as confidential provided that this Clause 1 shall not extend to any information which was rightfully in the possession of the Contractor prior to the award and commencement relating to this Service Contract or which is already in the public knowledge or becomes so at a future date (otherwise than as a result of a breach of this clause).

2. The Contractor shall indemnify and keep the Client fully and effectively indemnified against all costs, claims, demands, expenses and liabilities of whatsoever nature arising from or incurred by reason of any actions and/or claims made in respect of information subject to the Personal Data (Privacy) Ordinance (Cap 486) which action and/or claim would not have arisen but for the negligence or omission of the Contractor, any of its employees, Sub-contractors or agents (or any one acting on its/their behalf) in connection with the provision of the Services.

3. The Contractor hereby agrees that it will use such confidential information solely for the purposes of this Service Contract and that it will not, at any time before, during or after the completion, expiry or termination of this Service Contract use or allow to be used the same for any other purposes (whether directly or indirectly) without the Client prior written consent.

4. The Contractor undertakes to take all such security measures for the protection of the information, documentation and materials which it is obliged by Clause 1 to keep secret and treat as confidential as it takes for the protection of its own confidential or proprietary information, documentation and materials.

5. The Contractor shall ensure that each of its employees, agents, associates, Sub-contractors, consultants and any other persons engaged on any work in connection with this Service Contract are aware of and comply with the provisions of Clause 1 and the Contractor shall indemnify and keep the Client fully and effectively indemnified against all costs, claims, demands, expenses, loss, damage and liabilities which the Client may suffer, incur or sustain as a result of any breach of confidence (whether under this Service Contract or general law) by any such persons.

6. The Contractor further agrees that it will not at any time itself or through any subsidiary or agent use, sell, license, sub-license, create, develop or otherwise deal in any confidential information supplied to it by the Client or obtained while performing this Service Contract.

7. The Contractor shall promptly notify the Client and give the Client all reasonable assistance in connection with any proceedings which the Client may institute against any such persons pursuant to any of the provisions in this Appendix.

8. The provisions of this Appendix shall survive the expiry, completion or termination of this Service Contract (howsoever occasioned) and shall continue in full force and effect notwithstanding such expiry, completion or termination.

Annex E – Data Processor Review Checklist

The following checklist should be completed by the Section Coordinator as part of the annual data processor management review. The completed checklist should be submitted to the Data Protection Officer for review.

Part 1: Background information	
Section	
Name of data processor	
Purpose of engaging the data processor	
Brief description of personal data processed/accessed by the data processor	
Date of engagement with the data processor	

Part 2: Review of the Hong Kong Institution of Engineers (The HKIE)'s management of data processors		
Questions	**Yes/No**	**Remarks**
1) Do the contractual terms cover the HKIE's right to audit and inspect how the data processor handles and stores personal data?		
2) Do the contractual terms cover the data processor's obligation to report immediately to the HKIE for any loss of documents, security breaches or signs of abnormalities?		
3) Do the contractual terms cover the limitation of using or disclosing any personal data it receives or gains knowledge of that should be for a purpose which the personal data is entrusted to it?		
4) Do the contractual terms cover the subcontract arrangement limitations and arrangements?		
5) Do the contractual terms cover the timely return, destruction or deletion of personal data by the data processor?		
6) Do the contractual terms cover the data processor's obligations to adopt practicable means to protect the data entrusted to it (e.g. appropriate security measures, personal data protection policies and procedures, adequate training to relevant staff, cross-border data transfer arrangement)?		
7) Do the contractual terms cover the consequence for violation of the contract?		

8) Is the Section satisfied that the data processor had followed the contractual obligations in respect of personal data protection? If "Yes", please elaborate.		
9) If the answer to Q(8) above is "No", did the Section take any actions?		
10) Has the Section performed any scheduled audit/inspection on the data processor in the past three years (including surprise visit)? If the answer is "Yes", please state:- (a) the year of the audit/inspection (b) any irregularities identified; and (c) any remedial actions taken. If the answer is "No", please explain why an audit/inspection is not required.		
11) If audit/inspection was performed on the data processor this year, has the Section identified any irregularities? If "Yes", please state the details and the improvement measures taken by the data processor.		
12) Has any data breach incidents occurred which involved the data processor? If "Yes", please provide the corresponding Data Breach Information Sheet as attachment (please refer to Annex Q of this PMP Manual).		

Completed by (Section Coordinator)

Signature _____

Name _____

Post _____

Date _____

Reviewed by (Data Protection Officer)

Signature _____

Name _____

Post _____

Date _____

Reviewed by (Section Head)

Signature _____

Name _____

Post _____

Date _____

Annex F – Personal Data Inventory

Section	(a) Category of record	(b) Type of record containing personal data	(c) Items of personal data contained in the record	(d) Means of collection of the personal data	(e) Purpose of collecting and use of the personal data	(f) Retention period of the personal data	(g) Disclosure of personal data to any third parties incl. data processors (Yes/No)	(h) Possible location of transfer (e.g. cloud server location)	(i) *[Answer if response to (g) is Yes]* Names and relevant details of the third party(ies) to whom the personal data is disclosed	(j) Date of return or destruction by the data processor (if applicable)	(k) *[Answer if response to (g) is Yes]* Purpose of transferring to third parties	(l) *[Answer if response to (g) is Yes]* Purpose of disclosing the personal data (State whether the disclosure is specified in the PICS or made with the data subject's consent or in reliance of an exemption under Part 8 of the PDPO)	(m) Location of the personal data [Please refer to Note below]	(n) Security measures adopted	(o) Erasure schedule

Note:

Location of the personal data includes both physical and electronic location of files.

Completed by (Section Coordinator)

Signature _____

Name _____

Post _____

Date _____

Reviewed by (Data Protection Officer)

Signature _____

Name _____

Post _____

Date _____

Annex F – Personal Data Inventory

The following entries are only SAMPLES of completing the Personal Data Inventory.

Department	**(a) Category of record**	**(b) Type of record containing personal data**	**(c) Items of personal data contained in the record**	**(d) Means of collection of the personal data**	**(e) Purpose of collecting and use of the personal data**	**(f) Retention period of the personal data**	**(g) Disclosure of personal data to any third parties incl. data processors (Yes/No)**	**(h) Possible location of transfer (e.g. cloud server location)**	**(i)** *[Answer if response to (g) is Yes]* **Names and relevant details of the third party(ies) to whom the personal data is disclosed**	**(j) Date of return or destruction by the data processor (if applicable)**	**(k)** *[Answer if response to (g) is Yes]* **Purpose of transferring to third parties**	**(l)** *[Answer if response to (g) is Yes]* **Purpose of disclosing the personal data (State whether the disclosure is specified in the PICS or made with the data subject's consent or in reliance of an exemption under Part 8 of the PDPO)**	**(m) Location of the personal data [Please refer to Note below]**	**(n) Security measures adopted**	**(o) Erasure schedule**
Admin Department	*Employment related records*	*Leave files*	*Staff' information: - Name - HKID Card No. - Date of Birth*	*Through physical form*	*To facilitate the handling of individual officers' leave related matters*	*12 months after staff member has left the service*	*No*	*N/A*	*N/A*	*N/A*	*N/A*	*N/A*	*Physical: Filing cabinets in 13/F printing room Electronic : Filed in the shared drive of Admin Department*	*Physical: Filing cabinets are locked and the key is kept by organisation Admin personnel. Electronic: Filed in the shared drive of Admin Department and secured with password lock.*	*Files destruction exercise will be carried out in Q4 every year*
Marketing	*Membership records*	*Membership applications*	*Applicants' information: - Name - contact information (including address, mobile phone number and*	*Through physical and electronic membership application form*	*To process applications*	*1 year after cancellation of membership by the member*	*Yes*	*Within Hong Kong*	*data processor (ABC data input company)*	*Service provider will return the original copy within 3 days after completion of the task*	*To carry out data input*	*The personal data provided in the applications may be transferred or disclosed to (ABC data input company)*	*Physical: Filing cabinets of Departmental Coordinator of Marketing*	*Physical: Filing cabinets are locked and the key is kept by Departmental Coordinato*	*Files destruction exercise will be carried out in Q4 every year*

Department	(a) Category of record	(b) Type of record containing personal data	(c) Items of personal data contained in the record	(d) Means of collection of the personal data	(e) Purpose of collecting and use of the personal data	(f) Retention period of the personal data	(g) Disclosure of personal data to any third parties incl. data processors (Yes/No)	(h) Possible location of transfer (e.g. cloud server location)	(i) *[Answer if response to (g) is Yes]* Names and relevant details of the third party(ies) to whom the personal data is disclosed	(j) Date of return or destruction by the data processor (if applicable)	(k) *[Answer if response to (g) is Yes]* Purpose of transferring to third parties	(l) *[Answer if response to (g) is Yes]* Purpose of disclosing the personal data (State whether the disclosure is specified in the PICS or made with the data subject's consent or in reliance of an exemption under Part 8 of the PDPO)	(m) Location of the personal data [Please refer to Note below]	(n) Security measures adopted	(o) Erasure schedule
			email address)										*Deparmen t* *Electronic : Filed in the shared drive of Marketing Departme nt.*	*r of Marketing Departmen t Electronic: Filed in the shared drive of Marketing Departmen t and secured with password lock.*	

Note:

Location of the personal data includes both physical and electronic location of files.

Completed by (Departmental Coordinator)

Signature _____
Name _____
Post _____
Date _____

Reviewed by (Data Protection Officer)

Signature _____
Name _____
Post _____
Date _____

Annex G – Personal Data Records Disposal Guideline

When personal data is no longer required for the purpose for which it is or is to be used by the HKIE as the data user, it is the responsibility of the HKIE to erase the data or to prevent it from being kept longer than is necessary[21].

The respective Section should regularly review the time-expired records including both paper and electronic records (e.g. personal data kept in system) and identify time-expired records for timely disposal. A sample of the Personal Data Records Disposal Form is enclosed in Annex H for reference.

The Personal Data Records Disposal Process

There are six steps in the personal data records disposal process:

Step 1 – Review the personal data records for disposal

The respective Section should review the retention period of personal data records regularly and identify time-expired records for disposal based on the latest personal data inventory for their respective Section. The Section Head has to agree that the identified time-expired records are ready for disposal.

Time-expired records are ready for disposal?

- Yes: If the Section Head agrees that the identified time-expired records are ready for disposal, a record should be made for disposal.

- No: If there are valid reasons/needs to defer the disposal of time-expired records containing personal data, approval from its Section Head has to be obtained. Evidence of approval should be kept permanently by for record.

Step 2 –Record the disposal

After obtaining agreement for records disposal from the Section Head, the following information as far as practicable should be recorded for the disposal:

Before the records are disposed

- File Ref.
- File Name
- Personal Data Types
- Format (e.g. hardcopy, electronic, etc.)
- Location
- Any Backup Copies
- Reason for Disposal
- Method of Disposal

After the records are disposed

- Date of Disposal
- Staff Member who Oversees the Disposal Process

[21] Section 26 of the PDPO.

Care should be taken to ensure that the personal data disposal record itself does not contain personal identifiers. For the definition of personal identifier, please refer to Section 2 of this PMP Manual.

All copies of the personal data must be accounted for in the disposal exercise. This includes all photocopies, backup copies or digital copies of personal data. References should be made to the Personal Data Inventory to ensure that all copies of the personal data are accounted for.

Step 3 – Arrange the disposal of time-expired records

The respective Section should arrange for the disposal of the approved time-expired records with the designated contractor for collection and destruction of paper waste from the HKIE. In addition, the HKIE should arrange a responsible staff member to monitor the shred as far as practicable.

Step 4 – Retain all relevant disposal records

The respective Section should retain and keep all records relevant to the records disposal exercise permanently in the HKIE for record.

Annex H – Personal Data Records Disposal Form

Section: _____

File Ref.	File Name	Personal Data Types	Format (paper/ electronic)	Location	Any Backup Copies (Y/N/NA)	Reason for Disposal	Date of Disposal	Method of Disposal
e.g. A001	*File A*	*Customer information:* - *Name* - *Telephone Number* - *Email Address*	*Paper*	*Rm xxxx, ABC Centre*	*NA*	*Reached the retention period*		*Shred by contractor*

Annex I – Guideline for Handling of Personal Data Obtained over the Phone

Different types of personal data might be collected over the phone. The respective Section handling personal data over the phone should follow the procedures and requirements stipulated in this guideline. The respective Section handling personal data over the phone are advised to tailor their examples on purpose on collecting of personal data.

Operational needs on collection of personal data

To fulfil DPP1 - Data Collection Principle, the respective Section should consider their operational needs before collecting personal data. No personal data (including but not limited to name, HKID Card number, telephone number, address, email address) be collected unless there is an operational needs.

Below are some examples of collecting personal data with operational needs:

- *Identify a member/enquirer who inquire about his/her record*

  Personal data such as member/enquirer's name, company name, membership/application number, correspondence address, telephone number, and/or email address may be obtained to follow-up on his/her enquiries. The respective Section may disclose membership/application information to the member/enquirer. However, he/she should not further obtain the member/enquirer's HKID Card number in full. If required, part of the HKID Card number (e.g. the first or last few characters) can be obtained from the member/enquirer.

- *Contact an enquirer/a complainant who would like the HKIE to follow-up and reply on his/her enquiries/complaints.*

  Personal data such as *enquirer/complainant*'s name and telephone number may be obtained to follow up his/her enquiries/complaints. The respective Section may disclose the status of the enquiry/complaint to the enquirer/complainant. However, he/she should not further obtain the enquirer/complainant's date of birth, age and HKID Card number in full. If required, part of the HKID Card number (e.g. the first or last few characters) can be obtained from the member/enquirer.

Below are some examples where personal data should not be collected as there is no operational needs:

- *A customer who makes simple enquiries*

  No personal data should be collected if a enquirer makes simple enquiries (e.g. location of office). The respective Section may disclose information which is available to the public to reply the enquirer. However, no personal data should be disclosed to and collected from the enquirer.

- *A complainant who complains about the HKIE unless he/she would like the HKIE to follow-up on his/her complaints/enquiries*

  No personal data should be collected if a complainant makes a complaint (e.g. service issue), unless he/she requests for a feedback from the HKIE. The respective Section may disclose information which is available to the public to reply the complainant. However, no personal data should be disclosed to and collected from the complainant.

Due care should be imposed on collecting HKID Card number

The respective Section handling personal data over the phone should impose due care on collecting HKID Card number. According to the Code of Practice on the Identity Card Number and other Personal Identifiers issued by the Privacy Commissioner, HKID Card number is sensitive information, the HKIE should consider whether there may be any less privacy-intrusive alternatives (e.g. to verify the enquirer's name, address, telephone number instead of checking HKID Card number) to the collection of such number, and should wherever practicable give the individual the option to choose any such alternative in lieu of providing his identity card number before a data user seeks to collect from an individual his/her identity card number.

Inform the enquirer on the purpose of personal data collection

For cases that has identified the needs to collect personal data from enquirers, the following script should be used to , on or before collecting the data, inform the enquirer on the purpose of personal data collection. If necessary, respective Section, should tailor-made a standardised script based on the script below to inform the enquirer on the purpose of personal data collection.

Below is a suggested script to inform the enquirer on the purpose of personal data collection:

> *"To handle your enquiries/complaints (replace with the purpose), we will collect your personal data for the purpose. May I have your (e.g. name, telephone number and email address) please?"*
>
> "為處理閣下的查詢或投訴（或其他目的)，我們會收集閣下的個人資料。請提供閣下的(如；姓名、電話、地址及電郵地址)。"

Annex J– Hong Kong Identity Card Policy

Code of Practice on the Identity Card Number and other Personal Identifiers was first approved in December 1997 and revised in April 2016. The Code of Practice gives practical guidance to data users on the application of requirements to the collection of HKID Card number and HKID Card copies.

Non-compliance with the Code of Practice is not itself unlawful. However, it will give rise to a presumption against the party concerned in any proceedings involving an alleged breach of the Personal Data (Privacy) Ordinance and weigh against the part concerned in any case under investigation by the Privacy Commissioner.

(A) Collection of HKID Card number

Basic Position: No right to compel an individual to provide a HKID Card number unless authorised by law.

Step 1: Consider alternatives to collect HKID Card numbers
The respective Section should review their existing arrangements at least on an annual basis. The respective Section should consider to replace the collection of HKID Card numbers with any less privacy-intrusive alternatives.

Step 2: Check whether the ground for collection of HKID Card numbers is permitted by the Code of Practice
The HKIE is permitted to collect HKID Card number under any of the following circumstances:

(a) empowered or required by legislation, e.g. section 17K of the Immigration Ordinance (Cap. 115) requires organisation to keep a record of the HKID Card number for staff;
(b) required by section 58(1) of the PDPO, such as the prevention or deletion of crime, and the assessment or collection of any tax or duty;
(c) use for carrying out functions related to the operation of a tribunal or court;
(d) to advance the interests of the individual and prevent any third party from suffering a detriment; e.g. delivering mail to a special individual
(e) to safeguard the HKIE's interest against damage or loss that is more than trivial e.g. the potential loss of not returning money from users

Step 3: Check whether the HKID Card numbers collected is truly the HKID Card numbers of the individuals as far as practicable. In some cases, the individuals are required to make declaration that the information provided is true and correct.

(a) check against the HKID Card physically produced in person by the individual while collection of HKID Card number or before using the number for any purpose; or
(b) check against the HKID Card copy if the individual has been given options to either to provide a copy of HKID Card or to present the HKID Card in person;

Step 4: Check whether the use of HKID Card numbers is only for one of the purposes permitted by the Code of Practice

(a) to manage records relating to the individual that are held by the data user;
(b) to manage records related to the individual that were collected for the same particular purpose but were held by more than one data users; (e.g. several MPF trustees) (c) a purpose that the individual has expressed his voluntarily consent.

Step 5: Ensure the HKID Card numbers and the names of the HKID Card holders were not publicly displayed

The respective Section should check that HKID Card numbers are not displayed publicly with the names of the HKID Card holders. For example, the HKID Card number and names of HKID Card holders should not be printed on the staff card.

Step 6: Ensure the HKID Card numbers are not kept longer than necessary

The respective Section should ensure the retention period of HKID Card numbers are set not longer than necessary. The determination of the retention period should be made based on the previous practice of the HKIE.

(B) Collection of HKID Card copies

Basic Position: No right to compel an individual to provide a copy of a HKID Card unless authorised by law.

Step 1: Check whether the ground for collection of HKID Card numbers is permitted by the Code of Practice

The respective Section should ensure that the collection of HKID Card number is permitted under the Code if the requirements in Step 2 of (A) Collection of HKID Card number is fulfilled. Then, the respective Section should ensure the copy of HKID Card is further collected for any of the following purposes:

(a) to provide proof of compliance with any statutory requirement;
(b) to collect the copy which is included in any codes, court, rules, regulations or guidelines;
(c) to check against the HKID Card copy if the individual has been given options to either to provide a copy of HKID Card or to present the HKID Card in person;

Step 2: Check whether the ground for collection of HKID Card copies is not prohibited by the Code of Practice

(a) to safeguard against a clerical error of the name and HKID Card number of an individual;
(b) merely in anticipation of a prospective relationship with the individual;

Step 3: Check whether the copies of HKID Card collected is truly the copies of HKID Card of the individuals

(a) check against the HKID Card physically produced in person by the individual by the HKIE or by data processor; or
(b) if the HKID Card copies are received by post, the following actions should be taken:
    - mark “Checked to original” and date on the HKID Card copies and signed by the responsible staff member to ensure that HKID Card copies are not accepted unless they have been checked against the original HKID Card and no irregularity has been found.
    - mark “Collected without checking with the original” and date on the HKID Card copies and signed by the responsible staff member to remark that the copies have been collected without being checked against the HKID Card concerned.

Step 4: Check whether the use of HKID Card copies is only for one of the purposes permitted by the Code of Practice

(a) the purpose for which they were collected;
(b) a purpose to which the individual concerned has voluntarily given express consent; or (c) a purpose for which is exempted under the PDPO

Step 5: Ensure the HKID Card copies has adequate security safeguards during hold or transmit

(a) The respective Section should ensure the HKID Card copies are physically stored securely. (e.g. in a locked cabinet)

(b) The respective Section should ensure the transmission of the HKID Card copies in between Section and returning to the individual has adequate security safeguard. The HKIE should not transit a HKID Card copies unless it has taken all reasonably practicable steps to ensure that it is received only by the intended recipient. For example, when HKID Card copies is dispatched by mail, the envelope should be sealed so that the image of the HKID Card copies should not be visible through any window in the envelope.

(c) The responsible staff member should mark “copy” in the presence of the individual on the HKID Card copy across of entire image of the HKID Card.

Annex K – Information Security Guidelines for Portable Electronic Storage Devices

The HKIE is advised to consider the following issues before putting personal data of classified information onto portable electronic devices:

(a) **Understand the risks**

Devices such as USB flash memory sticks, Personal Data Assistants, mobile phones and MP3 music players are **risky places to store data**. They are small and easily lost or stolen. You should therefore be particularly cautious about storing data on these devices.

(b) **Confirm the need**

In general, data should only be made available on a "need-to-know" and "need-to-use" basis. You should consider whether you really need to store personal or classified data on such a device.

Consider **alternatives** such as:

- working on the data at the location where it was generated, rather than moving it to another location; and
- working with the use of an internal server with the necessary security protection.

You should **not** send personal or classified data through the Internet without having assessed the security risks and adopted the necessary protection measures.

(c) **Seek permission**

If you decide that you really need to store personal or classified data on a portable storage device, you must take steps to minimise the risk and consequences of data loss and seek prior permission on each occasion as appropriate. You should also keep clear and detailed records (including "when", "where", "what", "who", "how" and "why") in respect of the portable electronic devices which contain personal or classified data.

A request for storing personal/classified data on portable storage devices should be made to IT Section with the approval of Section Head.

(d) **Minimise the exposure**

You should only use a portable electronic device provided by organisation: never store personal or classified data on a personally owned device or PC.

You should **minimise the amount** of personal or classified data stored:

- do not store more data than you really need;
- if you are downloading from a database, make sure that you only extract the data fields and records that you absolutely need (**personal data** such as names and ID numbers **should be removed unless absolutely required**); and
- delete data from the device as soon as it no longer needs to be stored there.

(e) **Ensure safe custody and proper use of the data**

You should protect any personal or classified data stored on the device. Ways of achieving this include:

- **use a device that supports security protection**, including but not limited to passwords, encryption, biometrics (e.g. fingerprints).
- **ensure safe custody of the device**: make sure the device is stored/used in a location so that the device and the data are not susceptible to be stolen, copied or tampered with; and
- you should always consider making maximum use of the relevant security features offered by the application software.

(f) **Regular review**

Copying personal or classified data to a portable electronic storage device should be limited to one-off occasions, rather than being a regular practice. If regular copying is required, you should arrange with IT Section to provide a more secure way of transferring and accessing the data.

(g) **Incident reporting**

Any security incidents or data loss **should be reported immediately** to the HKIE's IT Section and the Chief Executive and Secretary and the Data Protection Officer.

Annex L – Guideline on the Safeguarding of Electronic Files Containing Personal Data

Staff should avoid creating and saving electronic files containing personal data (i.e. name, HKID Card number, address, telephone number, etc.) in the local drive of his/her own personal computer. The files should be stored in the encrypted share drive of the Section as far as possible. If this is inevitable due to operational needs, the following measures must be strictly adhered to:

- All electronic files containing personal data, whether exported or manually created on personal computers, must be password protected as far as possible;
- All electronic files containing personal data should be downloaded, copied or stored in the encrypted drive of the PC;
- The personal data inventory should be updated accordingly to include these electronic records containing personal data and their respective retention period and disposal policy; and
- All electronic files/records containing personal data should be deleted/disposed of immediately when there is no more operational needs to retain those data and/or the retention period is reached.

Annex M – Guideline on the Safeguarding of Hardcopy Documents Containing Personal Data

To fulfil the obligations under Data Protection Principle 4 in Schedule 1 to the PDPO, the HKIE, as a data user needs to take practical steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use, staff should as far as practicable adhere to the following measures when handling, processing and/or using personal data:

Hardcopy documents used in daily operations

a) All hardcopy files containing personal data should be handled in such a way as to restrict access only to those staff with operational needs to access them (on a need-to-know basis);

b) No documents containing personal data should be left unattended on desks, printers, fax machines, photocopiers and/or countertops; and

c) All hardcopy documents containing personal data should be kept at locked filing facility within the restricted office area when not in use, e.g. in a locked drawer or locked cabinet.

Hardcopy documents in transit

a) Documents containing personal data should be put into sealed envelopes and the sender should sign across the seal to ensure they are not opened during transit; and

b) The transit of documents containing personal data should be carried out by authorised staff members or an authorised service provider engaged by the HKIE.

Hardcopy documents to be destroyed

a) All documents containing confidential information to be destroyed should be stored in an enclosed and locked storage facility, e.g. nylon bags containing documents with personal data should be kept in an enclosed and locked storage facility before handled by third party servicing company; and

b) All hardcopy documents containing personal data should be disposed of immediately when the retention period is reached and should not be used as recycled paper.

Annex N – Privacy Policy Statement

Statement of Policy

1. [COMPANY/ORGANISATION] respects personal data privacy and is committed to implement and comply with the data protection principles and provisions under the Personal Data (Privacy) Ordinance (Cap. 486) ("PDPO").

Statement of Practices

Categories of Personal Data Held

2. [COMPANY/ORGANISATION] holds the following categories of personal data –

(i) **Employment-related records** which include data on job applications, personal particulars, education and qualifications, employment history, salary and allowances, participation in Mandatory Provident Fund, terms and conditions of service, housing and medical benefits, leave records, training and development, appraisal reports, conduct and discipline, etc.;

(ii) **General administrative records** which include personal data collected in connection with the office administration functions, records containing information supplied by data subjects and collected in connection with the handling of enquiries and complaints made to the [COMPANY/ORGANISATION], etc.;

(iii) **Customers records** which include personal data collected in the course of handling customers' membership applications, transactions, complaints and enquiries, etc.; and

(iv) **Other records** which include administrative and programme records containing personal data.

Main Purposes of Keeping Personal Data

3. The main purposes of keeping the personal data are as follows:

(i) **Employment-related records** are kept for a range of appointments and human resource management purposes, including postings and transfers, training and career development, performance appraisal and promotion, discipline, offer of benefits, etc.;

(ii) **General administrative records** are kept for the purposes of carrying out various office administration functions, responding to and taking follow-up actions on enquiries and complaints, etc.;

(iii) **Customer records** are kept for the purposes of handling customers' membership applications, transactions, complaints and enquiries, etc.; and

(iv) **Other records** are kept for various purposes, which vary according to the nature of the records, such as procurement of stores and equipment, organisation of activities, etc.

Practices of Personal Data Handling

4. The practices at (a) to (f) below are implemented to ensure that personal data held by [COMPANY/ORGANISATION] is handled in accordance with the data protection principles enshrined in the PDPO.

(a) Collection of personal data

5. When collecting personal data, [COMPANY/ORGANISATION] will satisfy itself that:

   (i) the purposes for which the data is collected are lawful and directly related to a function or activity of [COMPANY/ORGANISATION];
   (ii) the manner of collection is lawful and fair in the circumstances of the case; and

   (iii) the personal data collected is necessary but not excessive for the purpose(s) for which it is collected.

6. When [COMPANY/ORGANISATION] collects personal data from an individual, the individual will be provided with a Personal Information Collection Statement on or before the collection in an appropriate format and manner. Practicable steps will be taken to ensure that –

   (i) the data subject is informed of whether it is obligatory or voluntary for him/her to supply the data and, if obligatory, the consequences for him/her if he/she fails to do so; and

   (ii) the data subject is explicitly informed of the purpose for which his/her personal data is to be used, the classes of persons to whom the data may be transferred or disclosed, the rights of the data subject to request access to and correction of the data, and the contact details of the individual to whom any such request may be made.

(b) Accuracy and retention of personal data

7. Personal data collected and maintained by [COMPANY/ORGANISATION] shall be as accurate, complete, and up-to-date as is necessary for the purpose for which it is to be used.

8. [COMPANY/ORGANISATION] maintains a personal data inventory, which contains the kinds of personal data that [COMPANY/ORGANISATION] holds; the purposes for which the personal data is collected, used and disclosed; and how the personal data is stored. The personal data inventory will be reviewed on an annual basis to ensure that it is accurate and up-to-date.

9. Personal data will not be kept longer than necessary for the fulfilment of the purpose for which the data is collected or used. Personal data that is no longer required would be erased unless such erasure of personal data is prohibited under any law or it is in the public interest for the data not to be erased. Should there be a need to retain the personal data for statistical purposes, such data would be anonymised so that the individuals concerned could no longer be identified.

10. A destruction exercise on records containing personal data will be conducted as and when necessary and in accordance with [COMPANY/ORGANISATION] records management guidelines and procedures. Destruction of paper records would be carried out by irreversible means and electronic records would be cleared or destroyed from storage media before disposal by means of sanitisation or physical destruction.

(c) Use of personal data

11. All personal data collected will be used only for purposes, which are directly related to the discharge of [COMPANY's/ORGANISATION's] duties and responsibilities. Personal data collected may be transferred to third parties during the discharge of [COMPANY's/ORGANISATION's] functions when necessary. Relevant personal data may also be disclosed to other entities which are authorised to receive information for the purposes of law enforcement, prosecution or review of decisions. Data subjects would be informed of the possible transferees of their personal data when their personal data is collected.

12. If personal data is to be used for a purpose other than the purposes for which the data is collected, express prior consent preferred in writing would be sought from the data subject concerned. In seeking the data subject's consent, all practicable steps would be taken to ensure that (i) information provided to the data subject is clearly understandable and readable; and (ii) the data subject is informed that he/she is entitled to withhold his/her consent or withdraw his/her consent subsequently by giving notice in writing.

(d) Security of personal data

13. [COMPANY/ORGANISATION] observes strictly relevant security standards and regulations. Security arrangements will also be reviewed regularly to ensure that personal data is protected against loss and unauthorised or accidental access, use, disclosure, modification and erasure. The security arrangements adopted include but not limited to the following:

    (i) restriction of access to personal data on a "need-to-know" basis;

    (ii) regular review and enhancement of security measures for protection of personal data in the servers, user computers, transmission of electronic messages, etc.;

    (iii) regular change of passwords for IT facilities, accounting and personnel systems, etc.;

    (iv) encryption of all backup storage devices that are to be transported to offsite storage;

    (v) limited staff access rights to office areas storing confidential information; and

    (vi) provision of clear guidelines to staff as to the types of data that may or may not be disclosed to a phone enquirer and implementation of appropriate identity verification procedures to confirm the enquirer's identity.

(e) Transparency of the personal data policy and practices

14. [COMPANY/ORGANISATION's] privacy policy and practices can be found on [COMPANY/ORGANISATION's] website.

(f) Access to and correction of personal data

15. [COMPANY/ORGANISATION] recognises an individual's rights of access to and correction of his/her own personal data in accordance with the PDPO. To make a data access request, an individual should complete the form specified by the office of the Privacy Commissioner for Personal Data, which is available at http://www.pcpd.org.hk/english/publications/files/Dforme.pdf, and submit the completed form to [COMPANY/ORGANISATION] in any one of the following ways –

    [to be inserted with [COMPANY's/ORGANISATION's] contact details]
    By email: [email address]
    By fax: [fax number]
    By post or in person: [address]

16. When handling a data access or correction request, [COMPANY/ORGANISATION] will check the identity of the requester to ensure that he/she is the person legally entitled to make the data access or correction request.

17. [COMPANY/ORGANISATION] may impose a fee for the direct and necessary cost of complying with a data access request. [COMPANY/ORGANISATION] will clearly inform the requestor the amount to be charged.

18. [COMPANY/ORGANISATION] maintains a Register on Requests for Access to Personal Data recording the data access or correction requests received.

Incident Reporting and Breach Handling

19. A mechanism is set up for incident reporting and breach handling in case there is loss or leakage of personal data, or there is a reason to believe that the personal data held by [COMPANY/ORGANISATION] has been compromised.

Ongoing Monitoring and Review

20. [COMPANY/ORGANISATION] will keep the Privacy Policy and Practices under regular review. Officers responsible for handling personal data will attend relevant training courses to keep themselves updated of the latest personal data policies.

Annex O – Risk Assessment Questionnaire

As a part of the PMP periodic risk assessment (Section 3 – Part A – 2c – (a) of this PMP Manual), all or selected Section are required to complete the Risk Assessment Questionnaire to identify if there are any changes, new risks or threats that may impact the personal data protection measures of the HKIE.

Questions	**Yes/No (Y/N)**	**Number**	**Further actions required**
(a) New initiatives/projects developed or changes to existing activities involving personal data			
Q1. Have any new initiatives/projects or changes to existing activities involving personal data been launched or developed in the past 36 months or since the completion of your Section's last periodic risk assessment (whichever is later), which involve the collection, use and processing of personal data? (e.g. new personal data handling processes, launching of new systems, launching of consultation exercises, etc.) Please state the number of new initiative(s)/project(s) launched. *If the answer is "Yes", please proceed to **Q2 – Q4** below.* *If the answer is "No", please proceed to **(b) Data breach incidents**.*			
Q2. Has all personal data involved in the new initiative(s)/project(s) been updated in the personal data inventory? **[Note 1]**			If **no**, please update the personal data inventory immediately and submit the updates to the Data Protection Officer.
Q3. Has privacy impact assessment ("PIA") been conducted for the new initiative(s)/project(s) and submitted to the Data Protection Officer for review? Please state the name of the PIA(s) conducted. **[Note 2]**			If **due consideration was given before and there was no need to conduct a PIA**, please make sure the relevant justification is properly documented. If **a PIA is needed but not yet conducted**, please conduct the PIA in accordance with the Risk Assessment

Questions	Yes/No (Y/N)	Number	Further actions required
			Tools (for details, please refer to Section 3 – Part A – 2c of this PMP Manual).
Q4. If a PIA has been conducted, is the PIA still applicable? (i.e., were there any new changes, new privacy risks and means to address those risks, which require updates on the PIA?)			If **no**, please update the relevant documents (e.g. the PIA questionnaire) where applicable and submit them to the Data Protection Officer.
(b) Data breach incidents			
Q5. Has any data breach incident occurred in the past 36 months or since the completion of your Section's last periodic risk assessment (whichever is later)? **[Note 3]** *If the answer is "Yes", please proceed to **Q6 – Q7** below.* *If the answer is "No", please proceed to **(c) Complaints received**.*			
Q6. For each of the incidents, has a Data Breach Information Sheet been prepared? Has the Data Protection Officer reviewed the Information Sheet?			If **no**, please complete the data breach information sheet(s) (reference can be made to Annex Q) and submit it to the Data Protection Officer.
Q7. If Data Breach Information Sheets were prepared, has the data breach been mitigated?			If **no**, please update the data breach information sheet(s) and submit it to the Data Protection Officer.
(c) Complaints received			
Q8. Are there any complaint(s) about your Section's handling of personal data in the past 36 months or since the completion of your Section's last periodic risk assessment (whichever is later)? **[Note 4]** *If the answer is "Yes", please proceed to **Q9** below.* *If the answer is "No", please proceed to **(d) New data processor**.*			
Q9. Were all relevant complaints reported to the Data Protection Officer? Please state the reference number of the complaints received.			If **no**, please report the complaints to the Data Protection Officer immediately.

Questions	Yes/No (Y/N)	Number	Further actions required
(d) New data processor			
Q10. Has your Department engaged any new data processor(s) to handle personal data in the past 36 months or since the completion of your Section's last periodic risk assessment (whichever is later)? **[Note 5]** *If the answer is "Yes", please proceed to **Q11** below. If the answer is "No", please proceed to **Q12** below.*			
Q11. Has the Data Processor Review Checklist been completed?			If **no**, please complete the Data Processor Review Checklist (reference can be made to Annex E of this PMP Manual) and submit to the Data Protection Officer.
(e) Data disposal			
Q12. Has data disposal exercise been performed for all time-expired records within your Department?			If **no**, please arrange for data disposal according to [Records Disposal Guideline at Annex G].

Completed by (Section Coordinator)

Signature _____
Name _____
Post _____
Date _____

Reviewed by (Data Protection Officer)

Signature _____
Name _____
Post _____
Date _____

Note:

***[Note 1]**: Please refer to Section 3 – Part A – 2a: Personal Data Inventory of this PMP Manual.*

***[Note 2]**: Please refer to Section 3 – Part A – 2c: Risk Assessment Tools of this PMP Manual.*

***[Note 3]**: Please refer to Section 3 – Part A – 2e: Data Breach Handling Guidelines and Procedures of this PMP Manual.*

***[Note 4]**: Please refer to Annex D in this PMP Manual.*

***[Note 5]:** Please refer to Section 3 – Part A – 2f: Data Processor Management of this PMP Manual.*

Annex P – Privacy Impact Assessment ("PIA") Questionnaire

Part 1: Background information of the proposed change/project	
Name	
Section	
Staff member (Name and Post title)	
Expected date of implementation	
Description of the purpose of the personal data collection and the flow of handling personal data.	(In describing the purpose, please confirm whether the purpose is within one of the functions or activities of the HKIE)
Types of personal data to be collected (e.g. name, date of birth, Identity Card number, address, telephone number, etc.).	
Estimated number of data subjects from whom data is collected.	
Will any data processor(s) be involved? If **yes**, have the measures in the data process management been considered and carried out? Please elaborate on the measures to be taken. If no measures are to be taken, please elaborate on the justification.	*( ) Yes* *( ) No*
Will there be any transfer of personal data to a country outside of Hong Kong? If **yes**, please specify the destination(s) and the purpose(s) of such cross-border transfer. The answer should be as specific as practicable.	*( ) Yes* *( ) No*

Part 2: Privacy risks analysis		
Area	**PIA Question**	**Answers by Section**
Data Protection Principle ("DPP") 1 – Data Collection Principle • Personal data must be collected in a lawful and fair way, for a purpose directly related to a function or an activity of the data user. • All practicable steps shall be taken to notify the data subjects of the purpose of data collection and the classes of persons to whom the data may be transferred. • Data collected should be necessary but not excessive.	Will the data subjects be informed of the purpose of collecting their personal data? If **no**, please provide justifications.	*( ) Yes* *( ) No*
	Will the collection of personal data be on a minimum level to satisfy the purpose of collection (i.e. no excessive personal data is collected)? Please provide justifications on the purpose of collecting sensitive personal data below (including but not limited to): • Hong Kong Identity Card number / passport number[44] • Biometric data (e.g. fingerprints) [45]	*( ) Yes* *( ) No*
	Will the data subjects be informed, on or before the collection of the personal data, of whether the supply of the personal data is voluntary or obligatory?	*( ) Yes* *( ) No*
	Where it is obligatory for data subjects to supply the personal data, will the data subjects be informed of the consequence of not providing the personal data? If **yes**, please elaborate. If **no**, please provide justifications.	*( ) It is completely voluntary for the data subjects to supply their personal data.* *( ) Yes* *( ) No*
	Will the data subject be informed of whether the personal data collected will be transferred or disclosed to any third parties? If **yes**, please provide details of such third party. If **no**, please provide the reason.	*( ) Personal data will not be disclosed to any third parties. ( ) Yes* *( ) No*

[44] The "Code of Practice on The Identity Card Number and Other Personal Identifiers" issued by the Privacy Commissioner can be found at https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/picode_en.pdf

[45] The "Guidance on Collection and Use of Biometric Data" issued by the Privacy Commissioner can be found at https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pd

Part 2: Privacy risks analysis		
Area	**PIA Question**	**Answers by Section**
	If the personal data is to be transferred to any third party or data processor, will the data subjects be informed of the classes of persons to whom their personal data may be transferred or disclosed?	*( ) Personal data collected will not be transferred or disclosed to any third party.* *( ) Yes* *( ) No*
DPP2 – Data Accuracy and Retention Principle • All practicable steps shall be taken to ensure personal data is accurate and is not kept longer than necessary to fulfil the purpose for which it was originally collected.	Will there be any measures in place to ensure accuracy of the personal data organisation handles? If **yes,** please elaborate. If **no**, please justify.	*( ) Yes* *( ) No*
	What will be the retention period of the personal data? Please specify. Will there be any measures in place to ensure that personal data is not kept longer than necessary to fulfil the purpose of using the data? If **yes**, what are the measures? If **no**, please justify.	*Retention period: _____* *( ) Yes, data disposal exercise of time-expired records will be performed according to [Records Disposal Guideline at Annex G]* *( ) Yes, other measures: _____* *( ) No*
DPP3 – Data Use Principle • Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless the data user obtains from the data subject voluntary and explicit consent to use the data for a new purpose.	Will personal data be used only for the original purpose stated in the PICS? If **no**, what are the reasons?	*( ) Yes* *( ) No*
	Where the personal data will be used for a new purpose, has explicit consent been obtained from the data subjects? If **no**, please justify.	*( ) Personal data will not be used for purposes other than the original purposes for which it is collected.* *( ) Yes* *( ) No*

Part 2: Privacy risks analysis		
Area	**PIA Question**	**Answers by Section**
	Where personal data will be disclosed to a third party, will the third party be reminded of the purposes of such disclosure and its responsibility to confine the subsequent use of the data to these purposes? If **no**, please justify.	*( ) Personal data of data subjects will not be disclosed to a third party.* *( ) Yes* *( ) No*
	Where personal data will be disclosed to a third party, is the personal data disclosed to third party only necessary but not excessive? If **no**, please justify.	*( ) Personal data of data subjects will not be disclosed to a third party.* *( ) Yes* *( ) No*
DPP4 – Data Security Principle • Section Head needs to take all practicable steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.	Will there be any safeguard measures implemented to prevent unauthorised or accidental access, process, erasure, loss or use of personal data? If **yes**, please elaborate. If **no**, please justify.	*( ) Yes* *( ) No*
	Where data processor(s) will be involved, will there be any control in place to secure the personal data being handled by the third party? If **yes**, please elaborate. If **no**, please state the reason.	*( ) Third party data processor will not be involved.* *( ) Yes* *( ) No*
	Where data processor(s) will be involved, is the personal data disclosed to data processor only necessary but not excessive? If **no**, please justify.	*( ) Third party data processor will not be involved.* *( ) Yes* *( ) No*
	Where data processor(s) will be involved, will there be any contractual or other measures to ensure the personal data entrusted to the data processor is protected?	*( ) Third party data processor will not be involved.* *( ) Yes* *( ) No*

Part 2: Privacy risks analysis		
Area	**PIA Question**	**Answers by Section**
DPP5 – Openness Principle • Section Head must take all practicable steps to make known to the public the personal data policies and practices, types of personal data it holds and the main purposes for which it uses the data.	Is the existing Privacy Policy Statement on the HKIE website (a sample of the statement is enclosed in Annex N of this PMP Manual), regarding the kinds of personal data the HKIE holds, the main purposes of collecting and maintaining the personal data, and the HKIE's handling of personal data, still applicable? If **no**, please specify what update is needed.	*( ) Yes* *( ) No*
	Where there is a need to update the Privacy Policy Statement (a sample of the statement is enclosed in Annex N of this PMP Manual), has the Data Protection Officer been informed and will the updated Statement be uploaded to the website before the implementation of the change / the launch of the project? If **no**, please explain. **[Note]**	*( ) Yes, the Data Protection Officer has been informed and the updated Statement will be uploaded to website.* *( ) No update is required.*
DPP6 – Data Access and Correction Principle • Data subjects have the right to (i) request access to his/her own personal data held by the HKIE, and (ii) request the correction of the personal data supplied in a Data Access Request if it is inaccurate.	Will the data subjects be informed of their right to access and correct their personal data? If **no**, please justify.	*( ) Yes* *( ) No*
	Will the data subjects be informed of the post title and the address of the Personal Data Privacy Officer, i.e. the officer who is responsible for handling Data Access and Correction Requests? If **no**, please justify.	*( ) Yes* *( ) No*

Part 3: Potential risks and mitigation actions *Note: For any privacy risks identified, please describe the means to address the risks.* *Based on the results of Part 2, the respective Section should assess the potential risks identified in relation to each of the DPPs, especially those areas with "No" as answers. These risk areas should be highlighted in the table below with the respective mitigating measures identified. For those risk areas where no mitigating measures could be identified, the Section Head and the Data Protection Officer should be consulted and, where necessary, to assess the impact and whether the HKIE could accept such risk.*	
Potential risks identified	
Mitigation measures	

Completed by (Section Coordinator)		**Reviewed by (Data Protection Officer)**	
Signature	_____	Signature	_____
Name	_____	Name	_____
Post	_____	Post	_____
Date	_____	Date	_____

Note:
If there is a need to update the Privacy Policy Statement, the Data Protection Officer should be informed so that the Data Protection Officer can make necessary amendments to the Statement and arrange the upload of the updated version onto the HKIE's website. The respective Section should ensure that necessary amendments are made and the revised version is published before the implementation of the proposed change or project.

Annex P – Privacy Impact Assessment ("PIA") Questionnaire

The following case is only a SAMPLE of completing the PIA Questionnaire. In this example, a new complaint recording system is assumed to be launched.

Part 1: Background information of the proposed change/project	
Name	*Launch of a new complaint recording system*
Department	*[X Department]*
Subject officer (Name and Post title)	*[Name, Position]*
Expected date of implementation	*[Date]*
Description of the purpose of the personal data collection and the flow of handling personal data.	*The new complaint recording system will be used to record complaints made to* [COMPANY/ORGANISATION]*. Where a complainant launches a complaint and requests* [COMPANY/ORGANISATION] *to reply on the subject matter, personal data of the complainant (e.g. name and contact information) will be recorded in the new complaints recording system for further follow up actions. In case the complainant does not request a reply on the subject matter, personal data of the complainant will not be obtained. Further, the corresponding personal data of the complainant will be removed from the system after the complaint case is closed and when the personal information is no longer required.*
Types of personal data to be collected (e.g. name, date of birth, Identity Card number, address, telephone number, etc.).	*Name and contact number*
Estimated number of data subjects from whom data is collected.	*Approximately 10 data subjects per month*
Will any data processor(s) be involved? If **yes**, have the measures in the data process management been considered and carried out? Please elaborate on the measures to be taken. If no measures are to be taken, please elaborate on the justification.	*( ) Yes* *(✓) No* [COMPANY/ORGANISATION]
Will there be any transfer of personal data to a country outside of Hong Kong? If **yes**, please specify the destination(s) and the purpose(s) of such cross-border transfer. The answer should be as specific as practicable.	*( ) Yes* *(✓) No*

Part 2: Privacy risks analysis		
Area	**PIA Question**	**Answers by Team/Section**
DPP1 – Data Collection Principle • Personal data must be collected in a lawful and fair way, for a purpose directly related to a function or an activity of the data user. • All practicable steps shall be taken to notify the data subjects of the purpose of data collection and the classes of persons to whom the data may be transferred. • Data collected should be necessary but not excessive.	Will the data subjects be informed of the purpose of collecting their personal data? If **no**, please provide justifications.	*(√) Yes* *e.g. Personal Information Collection Statement will be provided to the complainant before the collection of their personal data. This statement could be found in the Contact Us webpage of* [COMPANY/ORGANISATION] *at* [COMPANY's/ORGANISATION's] website]. *( ) No*
	Will the collection of personal data be on a minimum level to satisfy the purpose of collection (i.e. no excessive personal data is collected)? Please provide justifications on the purpose of collecting sensitive personal data below (including but not limited to): • Hong Kong Identity Card number/passport number[22] • Biometric data (e.g. fingerprints)[23]	*(√) Yes* *e.g. Only the complainants' name and phone number will be collected.* *( ) No*
	Will the data subjects be informed, on or before the collection of the personal data, of whether the supply of the personal data is voluntary or obligatory?	*(√) Yes* *e.g. Personal Information Collection Statement* *( ) No*
	Where it is obligatory for data subjects to supply the personal data, will the data subjects be informed of the consequence of not providing the personal data? If **yes**, please elaborate. If **no**, please provide justifications.	*( ) It is completely voluntary for the data subjects to supply their personal data.* *(√) Yes* *A statement will be included in the Personal Information Collection Statement to inform the data subjects of their obligation in providing the data and the consequences if*

[22] The "Code of Practice on The Identity Card Number and Other Personal Identifiers" issued by the Privacy Commissioner can be found at https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/files/picode_en.pdf

[23] The "Guidance on Collection and Use of Biometric Data" issued by the Privacy Commissioner can be found at https://www.pcpd.org.hk/english/resources_centre/publications/files/GN_biometric_e.pdf

Part 2: Privacy risks analysis		
Area	**PIA Question**	**Answers by Team/Section**
		the data subjects fail to do so. This statement will be stated as "Please note that it is mandatory for you to provide personal data marked with asterisks. In the event that you do not provide such personal data, [COMPANY/ORGANISATION] may not be able to feedback to you the investigation result of your complaint." *( ) No*
	Will the data subject be informed of whether the personal data collected will be transferred or disclosed to any third parties? If **yes**, please provide details of such third party. If **no**, please provide the reason.	*( ) Personal data will not be disclosed to any third parties. (✓) Yes* *Consent will be obtained orally from the complainant when personal data collected may be transferred to third parties to handle the complaint cases. In particular, a complaint related to legal matters will be transferred to the responsible third party lawyer when necessary.* *( ) No*
	If the personal data is to be transferred to any third party or data processor, will the data subjects be informed of the classes of persons to whom their personal data may be transferred or disclosed?	*( ) Personal data collected will not be transferred or disclosed to any third party.* *(✓) Yes* *The personal data collected may be transferred to third parties to handle the complaint cases only when consent will be obtained from the complainant orally.* *( ) No*
DPP2 – Data Accuracy and Retention Principle • All practicable steps shall be taken to ensure personal data is accurate and is not kept longer than necessary to fulfil the purpose for which it was originally collected.	Will there be any measures in place to ensure accuracy of the personal data [COMPANY/ORGANISATION] handles? If **yes,** please elaborate. If **no**, please justify.	*(✓) Yes* *The personal data of complainant received by email are inputted by the subject officer in the complaint recording system. The personal data recorded in the system will be checked against the email received by other officer as independence review.* *( ) No*
	What will be the retention period of the personal data? Please specify.	*Retention period: N/A*

Part 2: Privacy risks analysis		
Area	**PIA Question**	**Answers by Team/Section**
	Will there be any measures in place to ensure that personal data is not kept longer than necessary to fulfil the purpose of using the data? If **yes**, what are the measures? If **no**, please justify.	*( ) Yes, data disposal exercise of time-expired records will be performed according to [Records Disposal Guideline at Annex G]* *( ) Yes, other measures:* _____ *(✓) No* *The retention policy is yet to be defined.*
DPP3 – Data Use Principle • Personal data must be used for the purpose for which the data is collected or for a directly related purpose, unless the data user obtains from the data subject voluntary and explicit consent to use the data for a new purpose.	Will personal data be used only for the original purpose stated in the PICS? If **no**, what are the reasons?	*( ) Yes* *(✓) No* *The personal data will be used for future analysis.*
	Where the personal data will be used for a new purpose, has explicit consent been obtained from the data subjects? If **no**, please justify.	*( ) Personal data will not be used for purposes other than the original purposes for which it is collected.* *(✓) Yes* *( ) No*
	Where personal data will be disclosed to a third party, will the third party be reminded of the purposes of such disclosure and its responsibility to confine the subsequent use of the data to these purposes? If **no**, please justify.	*( ) Personal data of data subjects will not be disclosed to a third party. (✓) Yes* *Third party will be reminded by* [COMPANY/ORGANISATION] *that the purpose of disclosing the personal data of the complainant will be bounded by handling the complaint only.* *( ) No*
	Where personal data will be disclosed to a third party, is the personal data disclosed to third party only necessary but not excessive? If **no**, please justify.	*( ) Personal data of data subjects will not be disclosed to a third party. (✓) Yes* *( ) No*
DPP4 – Data Security Principle • Team/Section Head needs to take practicable all steps to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use.	Will there be any safeguard measures implemented to prevent unauthorised or accidental access, process, erasure, loss or use of personal data? If **yes**, please elaborate. If **no**, please justify.	*(✓) Yes* *Safeguard measures are implemented according to the Guideline on the Safeguarding of Electronic Files Containing Personal Data. Access rights will only be granted to staff on a need-to-know basis.* *( ) No*

Part 2: Privacy risks analysis		
Area	**PIA Question**	**Answers by Team/Section**
	Where data processor(s) will be involved, will there be any control in place to secure the personal data being handled by the third party? If **yes**, please elaborate. If **no**, please state the reason.	*(√) Third party data processor will not be involved.* *( ) Yes* *( ) No*
	Where data processor(s) will be involved, is the personal data disclosed to data processor only necessary but not excessive? If **no**, please justify.	*(√) Third party data processor will not be involved.* *( ) Yes* *( ) No*
	Where data processor(s) will be involved, will there be any contractual or other measures to ensure the personal data entrusted to the data processor is protected?	*(√) Third party data processor will not be involved.* *( ) Yes* *( ) No*
DPP5 – Openness Principle • Team/Section Head must take all practicable steps to make known to the public [COMPANY/ORGANISATION's] personal data policies and practices, types of personal data it holds and the main purposes for which it uses the data.	Is the existing Privacy Policy Statement as stipulated in Annex N of this PMP Manual, regarding the kinds of personal data [COMPANY/ORGANISATION] holds, the main purposes of collecting and maintaining the personal data, and [COMPANY's/ORGANISATION's] handling of personal data, still applicable? If **no**, please specify what update is needed.	*(√) Yes* *( ) No*
	Where there is a need to update the Privacy Policy Statement as stipulated in Annex N of this PMP Manual, has the Data Protection Officer been informed and will the updated Statement be uploaded to the website before the implementation of the change/the launch of the project? If **no**, please explain. **[Note]**	*( ) Yes, the Data Protection Officer has been informed and the updated Statement will be uploaded to website.* *(√) No update is required.*

Part 2: Privacy risks analysis		
Area	**PIA Question**	**Answers by Team/Section**
DPP6 – Data Access and Correction Principle • Data subjects have the right to (i) request access to his/her own personal data held by [COMPANY/ORGANISATION] and (ii) reqest the correction of the personal data supplied in a Data Access Request if it is inaccurate.	Will the data subjects be informed of their right to access and correct their personal data? If **no**, please justify.	*(√) Yes* *Statement of rights of access and correction will be stated in the "Contact us" section of the website of* [COMPANY/ORGANISATION]. *( ) No*
	Will the data subjects be informed of the post title and the address of the Personal Data Privacy Officer, i.e. the officer who is responsible for handling Data Access and Correction Requests? If **no**, please justify.	*(√) Yes* *( ) No*

Part 3: Potential risks and mitigation actions *Note: For any privacy risks identified, please describe the means to address the risks.* *Based on the results of Part 2, the subject officer should assess the potential risks identified in relation to each of the DPPs, especially those areas with "No" as answers. These risk areas should be highlighted in the table below with the respective mitigating measures identified. For those risk areas where no mitigating measures could be identified, the subject officer should consult the Team/Section Head and the Data Protection Officer, where necessary, to assess the impact and whether [COMPANY/ORGANISATION] could accept such risk.*	
Potential risks identified	*The retention period of the personal data collected was not defined.* *The personal data collected will be used for future analysis and it was not mentioned in the PICS.*
Mitigation measures	*The personal data collected as part of the system implementation should be updated in the personal data inventory and the respective retention period should be defined.* *The PICS should be updated to inform the data subject of potential future analysis of personal data collected. The analysis of the personal data should be performed using anonymised data, where possible.*

Completed by (Departmental Coordinator)

Signature _____
Name _____
Post _____
Date _____

Reviewed by (Data Protection Officer)

Signature _____
Name _____
Post _____
Date _____

Note:
If there is a need to update the Privacy Policy Statement, the subject officer should inform the Data Protection Officer so that the Data Protection Officer can make necessary amendments to the Statement and upload the updated version onto [COMPANY/ORGANISATION's] website. It is the subject officer's responsibility to ensure that necessary amendments are made and the revised version is published before the implementation of the proposed change or project.

Annex Q – Data Breach Information Sheet

For guidelines on how to complete this information sheet, please refer to the Data Breach Handling Guidelines and Procedures (details can be found in Section 3 – Part A – 2e of the Privacy Management Programme (PMP) Manual).

SECTION	
INFORMATION OF THE BREACH	
General information of the breach	
Description of the breach	
Date and time of the breach (if known)	
Location of the breach *(e.g. which office, which computer server, etc.)*	
Date and time of discovering the breach	
How the breach is discovered *(e.g. discovered during routine system checking, known after being reported by the media, etc.)*	
Nature of the breach *(e.g. leakage, loss or, unauthorised use of personal data, etc.)*	
Cause of the breach (if known)	
Impact of the breach	
Types of data subjects affected *(e.g. staff, public, etc.)*	
Estimated number of data subjects affected *(Please state the respective number for each type of data subjects)*	

Types of personal data affected *(e.g. name, date of birth, Hong Kong Identity Card number, address, telephone number, etc.)*	
Medium holding the affected personal data *(e.g. physical folders, USB, hard disk, etc.)*	
If the personal data is held in electronic medium, is the data encrypted?	
DATA BREACH NOTIFICATION TO REGULATORY BODIES	
Are other regulatory bodies such as the Hong Kong Police Force or the office of the Privacy Commissioner for Personal Data notified of the data breach? If yes, please provide the date and details of each notification given.	
ACTIONS TAKEN / WILL BE TAKEN TO CONTAIN THE BREACH	
Brief description of actions <u>taken</u> to contain the breach	
If applicable, please evaluate the effectiveness of the abovementioned actions taken.	
Brief description of actions that <u>will be taken</u> to contain the breach	
RISK OF HARM	
Please assess here the potential harm to data subjects caused by the data breach and the extent of it.	

DATA BREACH NOTIFICATIONS TO DATA SUBJECTS AFFECTED	
Dates and details of the data breach notifications issued to data subjects affected by the breach	
If no data breach notification is issued/will be issued, please state here the consideration.	
INVESTIGATION RESULTS	
Cause(s) of the breach	
POST INCIDENT REVIEW (To be completed by the Data Protection Officer)	
Recommended improvement measures and the respective implementation date	
Date to review the effectiveness of the abovementioned improvement measures	

Relevant Training Materials:

Training Area	Training Material Source
Introduction of Personal Data (Privacy) Ordinance	• https://www.pcpd.org.hk/english/education_training/individuals/public_seminars/files/PDPO_eng_2019.pdf • https://www.pcpd.org.hk/tc_chi/education_training/individuals/public_seminars/files/PDPO_chi_2019.pdf • https://www.pcpd.org.hk/sc_chi/education_training/individuals/public_seminars/files/PDPO_chi_2019.pdf • https://www.pcpd.org.hk/misc/training/index.html • https://www.pcpd.org.hk/misc/sme_kit/tc_chi/index.html
PCPD Corporate Video	• https://youtu.be/oB8vnPzsyyo (English) • https://youtu.be/63xir_7sg-M (Cantonese) • https://youtu.be/WkbQBSie5bs (Putonghua)
Privacy Beyond Price Video	• http://www.rthk.hk/special/privacy2012/ • http://programme.rthk.hk/rthk/tv/programme.php?name=tv/privacybeyondprice2016
Six Data Protection Principles	• https://youtu.be/j6fO6JVGGHg (English) • https://youtu.be/86wYYT8173Q (Cantonese) • https://youtu.be/YnfFR5sRWw4 (Putonghua)
Handling Data Access Request	• https://www.pcpd.org.hk/misc/dpoc/files/dar_24032015.pdf
Personal Information Collection Statement	• https://www.pcpd.org.hk/misc/dpoc/files/pics_and_pps.pdf
Information Security and Data Privacy	• https://www.pcpd.org.hk/misc/dpoc/files/IT_Security_and_Data_Privacy_11032016.pdf
Direct Marketing	• https://www.pcpd.org.hk/mobileapps/files/Intro_DM.pdf • https://www.pcpd.org.hk/misc/dpoc/files/Sharing_on_Recent_Conviction_Cases_on_Direct_Marke.pdf
Introduction of the PMP	• https://www.pcpd.org.hk//tc_chi/resources_centre/publications/files/PMP_guide_c.pdf • https://www.pcpd.org.hk//english/resources_centre/publications/files/PMP_guide_e.pdf • https://www.pcpd.org.hk/misc/dpoc/files/briefing_pmp28052014.pdf
Newsletter / Updated news	• https://www.pcpd.org.hk/misc/dpoc/newsletter.html
Codes of Practice/ Guidelines	• https://www.pcpd.org.hk/english/data_privacy_law/code_of_practices/code.html • https://www.pcpd.org.hk/tc_chi/data_privacy_law/code_of_practices/code.html
Guidance Notes	• https://www.pcpd.org.hk/english/resources_centre/publications/guidance/guidance.html • https://www.pcpd.org.hk/tc_chi/resources_centre/publications/guidance/guidance.html
Information Leaflets	• https://www.pcpd.org.hk/english/resources_centre/publications/information_leaflet/information_leaflet.html • https://www.pcpd.org.hk/tc_chi/resources_centre/publications/information_leaflet/information_leaflet.html
Case Notes	• https://www.pcpd.org.hk/english/enforcement/case_notes/casenotes.php • https://www.pcpd.org.hk/tc_chi/enforcement/case_notes/casenotes.php

Document Revision Log

Date	Section	Description of Changes
10 January 2023	Part A-1a	Update of Section Coordinators
1 June 2022	Part A-1a	Change of job titles of staff members
1 November 2021	Relevant sections	Amendment of the footnote numbers
1 September 2021	All	Original issue