

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

Quick Reference Guide

The PMP Manual for the HKIE outlines the policies, practices, requirements and guidance relating to the handling of personal data at the HKIE. The HKIE should follow the PMP Manual when governing the collection, processing, maintenance and disposal of personal data. This Quick Reference Guide aims to provide an overview of the PMP Manual and to direct readers to the relevant sections of the Manual for further details.

The Personal Data (Privacy) Ordinance (“PDPO”) (Cap. 486) was enacted in 1995 and amended in 2012 and 2021. The objective of the PDPO is to protect the privacy of individuals in relation to personal data. The PDPO can be found at [Cap. 486 Personal Data \(Privacy\) Ordinance \(elegislation.gov.hk\)](http://www.elegislation.gov.hk/Cap.486).

	Page(s) of the Manual
PERSONAL DATA	
Personal data means any data –	5
(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, telephone number, address etc.	
DATA SUBJECT	
Data Subject refers to the living individual who is the subject of the personal data concerned.	5
DATA USER AND DATA PROCESSOR	
A data user is a person or organisation that either alone or jointly or in common with other persons or organisations, controls the collection, holding, processing or use of personal data.	5
A data processor is a person who processes personal data on behalf of another person, and does not process the data for any of the person’s own purposes.	
DATA PROTECTION PRINCIPLES (“DPPs”)	
The six DPPs represent the normative core of the PDPO and cover the life cycle of a piece of personal data.	6

DPP1 Data Collection Principle

When collecting personal data, the HKIE must satisfy itself that – 6, 15

- (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.

Personal Information Collection Statement (“PICS”) 39

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

- Statement of purpose
- Statement as to whether it is obligatory or voluntary for the individual to supply his/her personal data
- Statement of possible transferees
- Statement of rights of access and correction
- Contact person for requesting access or correction

Personal Data Inventory 13

The HKIE should be clear about what kinds of personal data it holds, where it is held and why it is collecting, using or disclosing personal data. An up-to-date personal data inventory should be maintained and reviewed annually.

Important note:

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. 15

Reference information:

[Annex A – Guidelines on the Preparation of Personal Information Collection Statement \(“PICS”\)](#) 39-45

[\(A template of Personal Information Collection Statement for Event is included\)](#) 40

[Annex I – Guidelines for Handling of Personal Data Obtained over the phone](#) 73-74

[Annex J – Hong Kong Identity Card Policy](#) 75-77

[Annex F – Personal Data Inventory](#) 67-69

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. Any time-expired records including electronic records identified should be disposed. 6, 13, 15

If a data processor is engaged, 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.

Reference information:

Annex G – Personal Data Records Disposal Guideline	70-71
Annex H – Personal Data Records Disposal Form	72
Section A-2f. Data Processor Management	32-34
Annex E – Templates of the Terms on Personal Data Protection in the Service Contract with Data Processor	58-64
Annex E – Data Processor Review Checklist	65-66

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. Personal data collected may only be transferred to third parties during the discharge of the HKIE’s functions when necessary. 6, 16

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.

DPP4 Data Security Principle

All practicable steps should be taken to safeguard personal data from unauthorised or accidental access, processing, erasure, loss or use. The security measures may include but not limited to the following: 7, 16, 17

- restriction of access to personal data on a “need-to-know” basis
- paper documents containing personal data must be stored in locked/secured location with limited access to authorised person
- adoption of password protecting and encrypting files to ensure that only the receiver with the password can access the file

All electronic files containing personal data should be stored in secured drive and the electronic files could be password protected.

Reference information:

[Annex K – Information Security Guidelines for Portable Electronic Storage Devices](#) 78-79

[Annex L – Guideline on the Safeguarding of Electronic Files Containing Personal Data](#) 80

[Annex M – Guideline on the Safeguarding of Hardcopy Documents Containing Personal Data](#) 81

DPP5 Openness Principle

All practicable steps should be taken 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. A Privacy Policy Statement is available on the HKIE website at [Privacy Policy | HKIE](#). 7, 17, 35, 82-85

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. 7, 17

A response must be made within 40 calendar days after receiving a data access or correction request.

Reference information:

[Annex B – Data Access and Correction Policy](#) 46-53

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. 26-31

When there is a data breach or when a data breach is suspected, prompt action should be taken to gather information and lessen the harm or damage that may be caused to the data subjects. The matter should be reported to the respective Section Head of the HKIE. The Section Head should then report to the Data Protection Officer and Chief Executive and Secretary.

Reference information:

[Annex Q – Data Breach Information Sheet](#) 102-104

Information in this Quick Reference Guide is mainly reproduced from the PMP Manual for the HKIE as a summary for reference. Readers should refer to the PMP Manual for the HKIE for details and full information.