

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited 香港臨床心理學家公會有限公司	Document No.	HKICP-ADM-GL-006-R0
	Guideline on Information Management and Information Security of HKICP	Issue Date	nn/nn/2018
Review Date			
Approved by			
		Page	1 of 14

Guideline on Information Management and Information Security of HKICP

Version	Effective Date
1.0	

Document Number	HKICP-ADM-GL-006-R0
Author	<<Post and Name>>
Custodian	<<Post and Name>>
Approved / Endorsed By	<<Respective Committees>>
Approval Date	DD/MM/YYYY

This document is only current as at the date of printing. Please refer to HKICP website for current version.

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited	Document No.	HKICP-ADM-GL-006-R0
	香港臨床心理學家公會有限公司	Issue Date	nn/nn/2018
	Guideline on Information Management and Information Security of HKICP	Review Date	
		Approved by	
		Page	3 of 14

Contents

	Page No.
1. Objective	4
2. Scope	4
3. Definition	4
4. Information Management	
4.1 Record Creation	4
4.2 Use and Manipulation of Records	5
4.3 Active Storage and Retention of Records	6
4.4 Record disposal	7
5. Information Security	
5.1 Personal Data	8
5.2 Personal Computer (PC) Security	9
5.3 Fax Machine	9
5.4 USB / removable storage	10
5.5 Email	10
6. Reference documents	10
7. Attachments	
7.1 Appendix 1: Record Retention Duration	12
7.2 Appendix 2: Document Disposal Record (Sample)	14

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited 香港臨床心理學家公會有限公司	Document No.	HKICP-ADM-GL-006-R0
	Guideline on Information Management and Information Security of HKICP	Issue Date	nn/nn/2018
		Review Date	
		Approved by	
	Page	4 of 14	

(Distribution list: This Policy shall be read by all staff and members of HKICP, Professional Council and its committees, and the general public.)

1. Objective

The objective of this document is to provide general guideline on information security and privacy for the systematic management of HKICP's information and records to tie in with the legislative requirements, organizational needs and operational environment.

2. Scope

This guideline is applicable to the management of administrative records as well as information of personal data created and maintained by HKICP.

3. Definition

Information can be stored as records in any physical format or medium, created or received in the course of official business and kept as evidence of policies, decisions, procedures, functions, activities and transactions.

4. Information Management

4.1 Record Creation

4.1.1 Paper records

Information may be created or received in the forms of:

- 4.1.1.1 Letter
- 4.1.1.2 Memorandum
- 4.1.1.3 Circular
- 4.1.1.4 Form
- 4.1.1.5 Minutes of meeting
- 4.1.1.6 Report
- 4.1.1.7 Publication

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited 香港臨床心理學家公會有限公司	Document No.	HKICP-ADM-GL-006-R0
	Guideline on Information Management and Information Security of HKICP	Issue Date	nn/nn/2018
		Review Date	
		Approved by	
	Page	5 of 14	

4.1.2 Electronic Records

4.1.2.1 For electronic records, the same rules applied.

4.1.2.2 However, for a series of email exchanges, only the final email with the exchanges in between needs to be retained.

4.2 Use and Manipulation of Records

4.2.1 Paper Records

4.2.1.1 Distributions of records

Distribution of paper records via photocopying should be minimized to reduce paper consumption. Paper record should either be circulated in its original format or scanned for distribution via email or posting in shared folder.

4.2.1.2 Filing

4.2.1.2.1 Filing is a process in which records of the same series on the subject are placed into a folder in accordance with the record index of the department.

4.2.1.2.2 To prevent duplication, only one set of file with all records on the subjects should be kept.

4.2.1.3 Record Indexing

All records must be stored in a systematic filing system with clear index for easy identification and retrieval.

4.2.1.4 Record Storage

4.2.1.4.1 The records should be properly stored in a clean, tidy and secure place free from water and fire hazards.

4.2.1.4.2 Storage equipment, such as file cabinets, drawers and racks, should be labeled properly for easy retrieval.

4.2.1.4.3 The access to confidential record storage areas should be limited to authorized personnel. Locks to store rooms or cabinets should be applied to ensure no unauthorized entry.

4.2.1.4.4 Active and inactive records should be separated to enhance retrieval efficiency and process for destruction.

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited 香港臨床心理學家公會有限公司	Document No.	HKICP-ADM-GL-006-R0
	Guideline on Information Management and Information Security of HKICP	Issue Date	nn/nn/2018
		Review Date	
		Approved by	
	Page	6 of 14	

4.2.1.5 Record Tracking

4.2.1.5.1 An updated record index should be kept (which covers information such as file reference number, title, storage location, date opened, date closed, date of destruction) as appropriate.

4.2.1.5.2 A system should be implemented to track the movement of records

4.2.1.6 Record Security Classification

Records which contain sensitive information should be classified as “Confidential” or “Restricted” depending on the degree of sensitivity. Specific file jacket should be used to hold classified papers.

4.2.1.7 Confidential Documents

4.2.1.7.1 A paper or document should be classified as ‘Confidential’ if the unauthorized disclosure of the information or material would be prejudicial to the interest of the HKICP.

4.2.1.7.2 The relevant executive should decide whether a file to be opened should be classified as “Confidential” and preferably with a pink folder, separating from other files.

4.2.1.7.3 All these files are accessible by staff on a need-to-know basis. Confidential files and documents should be kept under safe custody by the action officers responsible.

4.2.2 Electronic Records

4.2.2.1 Filing

Records should be filed in their final version and stored in such a manner that the document cannot be tampered thereafter.

4.2.2.2 Security for Electronic Records (See Pt. 5)

4.3 Active Storage and Retention of Records

4.3.1 Paper Records

4.3.1.1 Active files are those records frequently used for current business and therefore should be maintained in their origin office.

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited 香港臨床心理學家公會有限公司	Document No.	HKICP-ADM-GL-006-R0
	Guideline on Information Management and Information Security of HKICP	Issue Date	nn/nn/2018
		Review Date	
		Approved by	
	Page	7 of 14	

4.3.1.2 Files that have not been referred to in **2** years should be considered whether to be removed for remote storage if necessary (see Appendix 1 Record Retention Duration).

4.3.2 Electronic Records

Electronic records that are required for active reference should be posted in departmental shared folder or the intranet. Subject officer should conduct a regular review to ensure that the information posted is valid.

4.4 Record disposal

- 4.4.1 Classified records containing personal data should be retained and disposed of in accordance with relevant provisions of the Personal Data (Privacy) Ordinance.
- 4.4.2 Electronic records may be stored permanently in secured shared folder or corporate website with appropriate access control.
- 4.4.3 Inactive records should be included in a Bring-up (BU) system according to the minimum retention period specified. Destruction should be arranged for records that are no longer required.
- 4.4.4 The disposal of records should be properly authorized in advance. Endorsement on disposal of records shall be documented. Sample of the disposal document is attached for reference (Appendix 2).
- 4.4.5 Records retention and disposal schedules shall be reviewed regularly to cater for changing circumstances (e.g. a longer retention period due to a new statutory requirement).
- 4.4.6 For paper records that are classified for permanent retention, consideration should be given to permanent storage in an electronic format with the paper record destroyed where appropriate.
- 4.4.7 For destruction of confidential information and records with personal data, staff should take special measures to trash paper information. The HKICP will consider appointing a waste recycle company to dispose confidential documents if needed.
- 4.4.8 To safeguard against premature destruction of records having administrative, operational, legal, fiscal or archival value, destruction of records must be properly authorized by relevant subject officer and a record of disposal to be kept permanently

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited 香港臨床心理學家公會有限公司	Document No.	HKICP-ADM-GL-006-R0
	Guideline on Information Management and Information Security of HKICP	Issue Date	nn/nn/2018
		Review Date	
		Approved by	
	Page	8 of 14	

5. Information Security

5.1 Personal Data

5.1.1 Collection

The personal data provided in the application form and in handling any enquiry or complaint will be used by the HKICP and related Committees for the following purposes in accordance with the Personal Data (Privacy) Ordinance:

- 5.1.1.1 to process the application for registration,
- 5.1.1.2 to compile statistics,
- 5.1.1.3 to prepare, maintain and publish the register,
- 5.1.1.4 to process complaints or enquiries,
- 5.1.1.5 to send materials issued by HKICP to its registrants, and
- 5.1.1.6 any other legitimate purpose.

5.1.2 Disclosure of Personal Data to the Public

The name and registration number of registrants will be posted on the website of HKICP. The main purpose of publishing such information is to protect the public by creating a public record of persons who are accredited clinical psychologists and are entitled to practice the profession in Hong Kong.

5.1.3 Classes of Transferees

- 5.1.3.1 The personal data provided to HKICP are mainly for internal use but, if required, they may also be disclosed to other government departments, bureaus, agencies and authorities for the purposes mentioned above.
- 5.1.3.2 Apart from such disclosure, a person's data may only be disclosed to other parties where he/she has consented to such disclosure or where such disclosure is allowed under the Personal Data (Privacy) Ordinance (Cap 486).

5.1.4 Access to Personal Data

Applicants, registrants, or members of the public who have made enquiries or complaints, have the right to access and correct the personal data provided in accordance with sections 18 and 22 and Principle 6 of Schedule 1 of the Personal Data (Privacy) Ordinance (Cap 486). The right of access includes the right to obtain a copy of one's personal data provided during the occasions as

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited 香港臨床心理學家公會有限公司	Document No.	HKICP-ADM-GL-006-R0
	Guideline on Information Management and Information Security of HKICP	Issue Date	nn/nn/2018
		Review Date	
		Approved by	
	Page	9 of 14	

mentioned above. A fee may be imposed for complying with a data access request.

5.1.5 Disposal of Personal Data Records

The disposal of personal data records shall follow confidential waste handling. Confidential waste (with personal data records) shall be stored separately in locked or secured place, and separated from storage of general waste (refer to Pt. 4.4.7).

5.2 Personal Computer (PC) Security

5.2.1 Staff working in HKICP work sites should comply with the following security measures:

- 5.2.1.1 Lockdown the PC in open area using proper PC locks,
- 5.2.1.2 Close and lock windows or doors when leaving office,
- 5.2.1.3 Data in PC shall be accessed by authorized maintainer,
- 5.2.1.4 Use Screen Saver or blank the screen,
- 5.2.1.5 Don't share user IDs/ passwords of Systems or emails,
- 5.2.1.6 Use Strong Passwords and change them regularly.

5.2.2 Preventing Disaster with PCs

Data in PCs should be backed up regularly **at least once a month**.

5.2.3 Defending Against Viruses

- 5.2.3.1 Computer viruses can spread from system to system automatically. Extra care should be in place, such as installation of PC anti-virus software system with the latest virus definitions.
- 5.2.3.2 Ensure that any removable storage devices, including but not limited to USB flash drives, RAM disk, CD, DVD or floppy disk, coming into HKICP office are virus free, no matter where they come from.

5.3 Fax Machine

5.3.1 Do not use paper containing personal data as recycle paper for fax machine,

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited 香港臨床心理學家公會有限公司	Document No.	HKICP-ADM-GL-006-R0
	Guideline on Information Management and Information Security of HKICP	Issue Date	nn/nn/2018
		Review Date	
		Approved by	
		Page	10 of 14

5.3.2 Ensure recipient ready to collect before transmission.

5.4 USB / removable storage

5.4.1 Use encrypted USB / removable storage,

5.4.2 Do not store members' personal data in electronic devices unless with proper encryption,

5.4.3 Encrypt with 7-zip, or encryption by Microsoft,

5.4.4 Encrypt laptop hard disk.

5.5 Email

5.5.1 Do not send email containing confidential information without encryption,

5.5.2 For internal email, personal data (e.g. name + HKID) shall be removed,

5.5.3 If necessary, properly encrypt the data first,

5.5.4 Encryption password sent in SMS or over the phone (separate email if no other options),

5.5.5 Do not share your email accounts with others.

6. Reference Documents

6.1 Personal Data (Privacy) Ordinance (Cap.486) - e.g. timely destruction of personal data in accordance with Privacy Commissioner Office's Code of Practice on Human Resource Management; https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

6.2 Electronic Transactions Ordinance (Cap.553) - e.g. admissibility of electronic records in a court of law; <https://www.elegislation.gov.hk/hk/cap553!en>

6.3 Code on Access to Information - e.g. proper organization of records to facilitate their efficient retrieval to timely respond to public access requests. <http://www.access.gov.hk/en/home/index.html>

6.4 Limitation Ordinance (Cap.347) - e.g. retention of relevant records for the specified limitation periods to serve as evidence in possible legal proceedings; <https://www.elegislation.gov.hk/hk/cap347>

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited 香港臨床心理學家公會有限公司	Document No.	HKICP-ADM-GL-006-R0
	Guideline on Information Management and Information Security of HKICP	Issue Date	nn/nn/2018
		Review Date	
		Approved by	
	Page	11 of 14	

6.5 Evidence Ordinance (Cap. 8) – e.g. proper keeping of records to ensure its legal <https://www.elegislation.gov.hk/hk/cap8!en>

6.6 InfoSec Website Government of HKSAR
<https://www.infosec.gov.hk/english/main.html>

6.7 HA's Policy on Information Security and Privacy(ITCir1-2009)

6.8 Government Records Services
<http://www.grs.gov.hk/en/>

6.9 Copyright ordinance
https://www.infosec.gov.hk/english/ordinances/ordinances_copyright.html

6.10 HA Information and Security Guide
<http://infosec.home/PoliciesAndGuidelines/InformationSecurityAndPrivacyPracticalGuide.aspxH>

6.11 HKICP Information management and security policy

7. Attachments

7.1 Appendix 1: Record Retention Duration

7.2 Appendix 2: Document Disposal Record (Sample)

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited 香港臨床心理學家公會有限公司	Document No.	HKICP-ADM-GL-006-R0
	Guideline on Information Management and Information Security of HKICP	Issue Date	nn/nn/2018
		Review Date	
		Approved by	
	Page	12 of 14	

Appendix 1: Record Retention Duration

Description	Minimum Retention Period	Action After Retention Period
A. General		
1. Routine correspondence	3 years	Destruction
2. Director's meeting minutes	Permanent	
3. Sub-committee meeting minutes	7 years	To be reviewed by subject officer(s)
4. Register of Registrants	Permanent	
5. Complaint and Appeal	Permanent	
B. Finance Records		
1. Policy	7 years	To be reviewed by subject officer(s)
2. All types of ledgers and accounting records in support of the preparation of financial statements (e.g. journal vouchers, payment vouchers, cash and bank records, receipt records, asset records, etc)	7 years	To be reviewed by subject officer(s)
Description	Minimum Retention	Action After Retention

[LOGO]	Hong Kong Institute of Clinical Psychologists Limited 香港臨床心理學家公會有限公司	Document No.	HKICP-ADM-GL-006-R0
	Guideline on Information Management and Information Security of HKICP	Issue Date	nn/nn/2018
		Review Date	
		Approved by	
	Page	13 of 14	

	Period	Period
3. Accounting records other than (2) above such as daily transaction reports generated from the financial systems, demand note, etc.	2 years	To be reviewed by subject officer(s)
C. Procurement and Materials Management		
1. Tender/contract document		
1.1 successful tender	3 years	To be reviewed by subject officer(s)
1.2 unsuccessful tender	3 years	
D. Human Resources		
1. Policy	Permanent	To be reviewed by subject officer(s)
2. Daily operation documents	3 years	
3. Human resources records with personal data	In accordance with Personal Data(Privacy) Ordinance	

