

Hong Kong Institute of Speech Therapists Limited	Document No.	HKIST-A-IMP-v2
	Issue Date	25/08/2022
Information Management and Information Security Policy	Review Date	24/08/2024
	Page	1 of 3

# Information Management and Information Security Policy

Version	Effective Date
1.0	17/09/2017
2.0	25/08/2022

<b>Document Number</b>	<b>HKIST-A-IMP-v2</b>
<b>Author</b>	<b>HKIST Director</b>
<b>Custodian</b>	<b>HKIST Director</b>
<b>Approved / Endorsed By</b>	<b>HKIST Board of Directors</b>
<b>Approval Date</b>	<b>25/08/2022</b>

Hong Kong Institute of Speech Therapists Limited	Document No.	HKIST-A-IMP-v2
	Issue Date	25/08/2022
Information Management and Information Security Policy	Review Date	24/08/2024
	Page	2 of 3

## 1.0 Purpose

The functions of the Hong Kong Institute of Speech Therapists Limited (HKIST) involves the handling of a significant amount of personal data. This includes information related to the application for accreditation, continuing education and disciplinary proceedings of its accredited registrants. Preserving the privacy of the personal data of the HKIST registrants is of utmost importance. It is therefore essential to ensure that information systems were appropriately managed and information security measures are in place.

## 2.0 Scope

All employees and members of the HKIST Board of Directors, Professional Council and its committees who are involved in the handling and processing personal data of accredited speech therapists should comply with this information management and security policy, and should be alert in the protection of security and privacy of personal data. Relevant education and training for all employees and members of HKIST will be regularly conducted to ensure a firm understanding of this policy, as well as the related procedures.

## 3.0 Policy Statement

The HKIST is committed to the management of risks associated with the management of information systems and the reduction of information technology (IT) security incidents. This policy provides the governance framework for information management and security of the HKIST. It mandates the effective protection of security and privacy of personal information with respect to its collection, use, storage (all media), access, extraction, transmission and disposal. All identifiable personal information should be handled with the highest level of security and privacy protection.

## 4.0 Principles

This Policy ensures that personal information:

- 4.1 be properly safeguarded to maintain confidentiality, integrity and availability,
- 4.2 be protected according to the Personal Data (Privacy) Ordinance. The ordinance has laid down the following data protection principles:
  - 4.2.1 Personal data should be obtained and processed lawfully and fairly
  - 4.2.2 Personal data should be accurate, up-to-date and kept no longer than necessary
  - 4.2.3 Personal data should be used for the purposes for which they were collected, with consent obtained from the data owner
  - 4.2.4 Appropriate security measures should be applied to personal data

Hong Kong Institute of Speech Therapists Limited	Document No.	HKIST-A-IMP-v2
	Issue Date	25/08/2022
Information Management and Information Security Policy	Review Date	24/08/2024
	Page	3 of 3

- 4.2.5 Policies and practices on how personal data are handled should be generally available
- 4.2.6 Provide channels for data subjects to have rights of access to and correction of their personal data
- 4.3 be accessed on a need-to-know basis, and the registrants could decide on which personal data to be disclosed to the public upon application for accreditation.

## 5.0 Secure Information Management

To comply with the above principles, effective procedures and measures, both administrative and technological, should be formulated, implemented and maintained. The HKIST will ensure that:

- 5.1 building and entry controls for areas used in the processing and storage of security classified information are established and maintained
- 5.2 all computers that store or process the information collected are in Secure Areas with control mechanisms in place to restrict access to authorized personnel only
- 5.3 Policies, procedures and processes are implemented to monitor and protect the use and/or maintenance of information systems
- 5.4 Policies, procedures and processes are implemented for the secure disposal or reuse of information systems

## 6.0 Security Incident Management

For security and privacy violations and breaches involving personal data, an effective incident reporting and handling system must be in place to ensure speedy investigative and remedial actions in the interest of the data subjects and the community. Disciplinary and legal actions may be taken against the person responsible for deliberate violations and breaches. To minimize potential and consequential damages, reporting of possible security and privacy breaches is encouraged.