



Aga Khan University Hospital

Document Title:	Acceptable Use of ICT Assets		
Department / Division:	Information Communications Technology (ICT)		
Approved By:		Document Reference/Policy No.:	ADM-P-010
Chief Information Officer		Issuance Date:	07 December 2020
		Revision Date:	24 May 2024
		Revision No.:	3.0
		Number of Pages:	7

1.0 Policy Statement: AKU prioritizes the secure use of ICT assets. Users are granted authorized access based on their roles, and strict adherence to the policy statements to ensure the confidentiality, integrity, and availability of information. Robust measures, including strong password practices, access control mechanisms and controlled software installations, are enforced to maintain the integrity and security of our network.

2.0 Terms and Definitions:

2.1 ISO: International Organization for Standardization.

2.2 AKU: Aga Khan University.

2.3 ICT: Information Communications Technology.

3.0 Purpose: The purpose of this policy is to establish acceptable use of AKU ICT assets within reasonable business needs.

4.0 Scope: This policy applies to all AKU employees, contractors, and vendors that have been provided with an ICT resource or have been allowed to use their resource to be connected to the AKU network. This includes and is not limited to, all related documentation, software, hardware, infrastructure, and information. The scope of this policy is applicable for all AKU domestic and global locations. In case of any specific local country regulations not addressed by this policy, the AKU local office will develop and maintain local policy to comply with the local regulatory requirements with the approval of Head of Information Security and Chief Information Officer.

5.0 Responsibility: Responsibility to follow the Acceptable Use of ICT Assets policy lies with all AKU employees, contractors, and vendors who have been granted access to the ICT resources.

6.0 Process /Procedure:

- 6.1 All ICT assets are the data, applications and operating systems, communications networks, and hardware used in AKU operations. Acceptable use of ICT assets shall be consistent with AKU's mission of education, research, service, and patient care, and must be legal, ethical, and honest. They must be used in an acceptable and appropriate manner and in accordance with the listed policy statements.
 - 6.1.1 All users must comply with all laws, regulations, or contractual obligations applicable to ICT assets. If a user has any question about what may be an acceptable use of data, applications, devices, or ICT processing facilities, they should contact the ICT Support Desk or their manager for further directions.
 - 6.1.2 All ICT assets belong to AKU and are designated for conducting AKU business, interacting with internal and external networks, and accomplishing AKU's operational objectives. Usage of ICT assets is restricted to authorized personnel only.
 - 6.1.3 Users utilizing ICT resources are subject to having their activities monitored by system or security personnel without any specific notice.
 - 6.1.4 Limited personal use of the ICT assets is allowed, provided such use is within the parameters of the information security policy contained herein. AKU expects personal use to be reasonable and reserves the right to limit personal use with or without cause or notice at any time.
- 6.2 Personal use may be terminated or restricted when such use:
 - 6.2.1 Conflicts with an employee's ability to perform their job.
 - 6.2.2 Places AKU ICT systems or data at risk in any way, regardless of the degree of risk.
 - 6.2.3 Uses large amounts of ICT resources or hinders the performance of any system.
 - 6.2.4 Does not conform to AKU's values or mission; or
 - 6.2.5 Violates any part of the Information Security Policy or associated standards or procedures.
- 6.3 AKU does not imply or express any warranty regarding its ICT assets or suitability for use for personal purposes and is not liable for any damages, consequential or otherwise, incurred by any user when using AKU ICT assets for personal purposes.
- 6.4 Storage of personal information on AKU system or devices will be considered the property of AKU and managed as the organization sees fit. AKU is not responsible for ensuring the confidentiality of such personal information. Without notice, AKU may delete, move, copy, or remove any personal information as deemed necessary.

- 6.5 AKU does not imply or express any warranty regarding its ICT assets or suitability for use for personal purposes and is not liable for any damages, consequential or otherwise, incurred by any user when using company ICT assets for personal purposes.
- 6.6 The following are discouraged except where required:
 - 6.6.1 Access or view social media sites during work hours.
 - 6.6.2 Personal use of AKU ICT assets and applications is forbidden during work hours.
 - 6.6.3 Accessing personal email through webmail interfaces hosted on personal email sites.
 - 6.6.4 Streaming non-work-related video, radio, or music.
 - 6.6.5 Establishing or using external storage areas, such as Drop Box etc.
- 6.7 The following activities are strictly prohibited:
 - 6.7.1 Disguising one's identity, the identity of their account or the system(s) they use.
 - 6.7.2 Sharing passwords and any other secret authentication information.
 - 6.7.3 Using another user's credentials.
 - 6.7.4 Impersonating another user or organization.
 - 6.7.5 Unless authorized to do so, using AKUs name, logos, trademarks, service marks, or any other information that would cause others to mistake the user as acting on behalf of AKU.
 - 6.7.6 Accessing AKU IPs to host personal or business domains.
 - 6.7.7 Accessing another's computer, device, or data without authorization.
 - 6.7.8 Sharing and disclosing sensitive information outside AKU is strictly prohibited.
 - 6.7.9 Reading, copying, altering, or deleting another user's data, except as allowed upon departure from the company or with permission from AKU's legal counsel.
 - 6.7.10 Copying or violating the intellectual property rights of any person or company protected by copyright, trade secret, patent, or other similar rights, without express permission. This includes copying software in violation of any software license agreement. (In the case of authorized copying of intellectual property or protected data, copies will only be made to AKU-approved equipment.)
 - 6.7.11 Installing, downloading, or distributing "pirated" software or any other software not specifically approved by AKU.
 - 6.7.12 Installing any equipment on AKU's network; installations are restricted to authorized devices/hardware and must be performed by AKU's ICT personnel.

- 6.7.13 Obtaining files from unauthorized external networks.
- 6.7.14 Sending, placing, or keeping any AKU data on any unapproved personal equipment or storage devices, in personal email, or on any site or media not owned by AKU.
- 6.7.15 Committing acts that would disrupt or interfere with the legitimate activities of other users.
- 6.7.16 Using AKU's ICT Resources to possess, distribute, or send unlawful communications or information. Such information or communications may include, but are not limited to, threats of violence or destruction of property, obscenity, child pornography, harassment (as defined by law), discrimination, or participating or facilitating the same of others, or the furtherance of other illegal or fraudulent activities.
- 6.7.17 Sending unsolicited email messages, including the sending of "junk mail," "phishing" or other advertised material to individuals who did not specifically request it (email spam).
- 6.7.18 Unauthorized use of or forging of email header information.
- 6.7.19 Creating or forwarding "chain letters," Ponzi or other pyramid schemes of any type.
- 6.7.20 Posting identical or similar non-business-related messages to blogs or large numbers of Usenet newsgroups (newsgroup spam).
- 6.7.21 Attempting to bypass or circumvent AKU's security safeguards.
- 6.7.22 Attempting to degrade the performance of any AKU system.
- 6.7.23 Accessing content inappropriate for the workplace. Such content shall include, but not be limited to:
 - i. Pornographic and obscene material.
 - ii. Gambling, gaming, dating sites.
 - iii. Chat rooms.
 - iv. Sites with violent content.
 - v. Sites with content focused on sexual interests and activities.
 - vi. Sites with pirated or peer-to-peer content.
- 6.8 AKU may contact law enforcement authorities to investigate any matter at its sole discretion without notifying the user. Users must immediately report any suspected or known violations of the Information Security Policy or associated standards, or procedures, computer performance issues or system or service weaknesses, or computer hardware or

software malfunctions by contacting the ICT Service Desk. All such reports shall be documented by the ICT Service Desk.

6.9 Acceptable use of the AKU email facility includes the following:

6.9.1 The AKU email system must not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

6.9.2 It is strictly prohibited to use AKU emails for activities including but not limited to:

- i. Using email for conducting personal business.
- ii. Using email for purposes of political lobbying or campaigning.
- iii. Violating copyright laws by inappropriately distributing protected works.
- iv. Posing as anyone other than oneself when sending email.
- v. The unauthorized use of email software.
- vi. Revealing your account password to others or allowing use of your account by others.
- vii. Providing unauthorized information including email addresses to parties outside the University.
- viii. Disclosure or circulation of any AKU emails outside of AKU which potentially may have a negative impact on AKU operations or reputation or cast aspersions on the integrity or character of someone employed in AKU.
- ix. Sending or forwarding chain letters.
- x. Sending unsolicited messages to large groups except as required to conduct AKU business.
- xi. Messages intended for groups of personnel, for example, congratulatory or obituary notes, should only be sent with manager approval.
- xii. Sending or forwarding email that is likely to contain computer viruses.
- xiii. Sending or forwarding email that contains videos, audio and presentations files greater than 35MB unless explicitly authorized to do so. Users must not forward, store or receive AKU data on non-AKU email addresses including, but not limited to, Gmail, Hotmail and Yahoo.
- xiv. Exposing large number of AKU email addresses on mass emails. Such an audience should be addressed by using the email bcc function.

- 6.10 Social Media: Use of WhatsApp, Facebook Messenger, Hangout, Skype or any other social media platform to share AKU's internal information including but not limited to patients, students, or employees personal, healthcare or any other sensitive information is strictly against AKU ICT policy, unless prior approvals have been granted by the Chief Information Officer. Microsoft Teams is the approved and secure application for calls, chats, and for sharing of such information. This does not apply to the public information, which is usually available on AKU website and social media channels. Please refer AKU Social Media policy for details (<https://one.aku.edu/communications/Pages/social-media-policy.aspx>)
- 6.11 Return of ICT Assets: All AKU *regular and contractual* employees shall return all ICT assets provided to them upon termination of their employment.
- 6.12 Disciplinary Action: A breach of this policy may result in disciplinary action, which could lead to dismissal.

7.0 Compliance Reference:

7.1 ISO/IEC 27001:2013 standard, Clause A.7.2 - Information Security Policy.

7.2 ISO/IEC 27001:2013 standard, Clause A.7.3 - Information Security Objectives.

7.3 ISO/IEC 27001:2013 standard, Clause A.8 - Asset Management.

7.4 ISO/IEC 27001:2013 standard, Clause A.9 - Access Control.

7.5 ISO/IEC 27001:2013 standard, Clause A.7.2.2 - Information Security Awareness, Education, and Training.

8.0 Measure of Compliance: Upon joining AKU, employees are required to affirm their agreement to Acceptable Use of ICT assets policy, before discharging their roles and responsibilities. This commitment will better ensure compliance with this policy.

9.0 Reference: This policy satisfies the following requirement of the Standard:

Clause Reference	Name of the Clause	Control reference	Name of control	Name of the Standard
-	-	A.8.1.3	Acceptable use of assets	ISO/IEC 27001:2013

10.0 Related Institutional Documents: [AKU Social Media Policy](#)

11.0 Annexure: For additional guidance refer the [Information Security Policy Manual \(ADM-P-024\)](#)

12.0 Author(s)

Name	Designation
Suneel Kumar Panjwani	Head of Information Security

Samra Sabir	Information Security Analyst
Atif Ali Soomro	Information Security Analyst
Saad Ameen	Information Security Specialist

13.0 Key Searchable Terms: Assets, Information Security, Prohibited, Acceptable Use.

14.0 Documents Change Record:

Review #	Review Date (dd-mm-yyyy)	Description of Change	Identification of Change
03	24-05-2024	Reviewed and updated the document in accordance with the latest policy document template.	-