Aga Khan University Hospital

Document Title:	Bring Your Own Device (BYOD)		
Department / Division:	Information Communications Technology (ICT)		
Approved By:		**Document Reference/Policy No.:**	ADM-P-027
Chief Information Officer		**Issuance Date:**	27 May 2021
		Revision Date:	24 May 2024
		Revision No.:	2.0
		Number of Pages:	4

1.0 Policy Statement: This policy provides leading practices to protect data, applications, and the associated infrastructure of mobile devices.

2.0 Terms and Definitions:

2.1 ISO: International Organization for Standardization

2.2 AKU: Aga Khan University

2.3 ICT: Information Communications Technology

2.4 BYOD: Bring Your Own Device

3.0 Purpose: This document outlines the Aga Khan University's (AKU) policy on Bring Your Own Device (BYOD). The purpose of the document is to deliver a set of guidelines to protect the integrity of AKU network when a user connects a personal device to AKU network. Also, it aims to reduce risks which may arise from the personal device being lost, stolen, used, or exploited in such a way to take advantage of you or the University.

4.0 Scope: This policy is applicable to all users. This includes students, faculty members, administrative staff, medical practitioners, and all other employees (contractual & permanent) using personally owned devices such as smart phones, tablet laptops and similar equipment's to store, access, carry, transmit, receive or use AKU information or data, whether at home, on campus or while travelling. 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: It is the responsibility of all AKU's users including volunteers, students, faculty members, and staff.

6.0 Policy Content:

6.1 Users must set and use strong password or pin code on their devices and comply with AKU Password Policy. Make sure that the password is kept secret and not shared with anyone.

6.2 Users must not use any pirated software or operating system on their devices which will be connected to AKU network.

6.3 Users must ensure that their devices are up to date. This includes operating systems, applications, anti-virus software and security updates. Users must not use their device for AKU work if their machines are outdated and no longer supported.

6.4 Users must ensure that devices should be locked automatically when inactive for more than 15 minutes.

6.5 Carrying official data on personal storage devices is not allowed. If it is necessary to carry the data on personal devices, the user must ensure that the device is encrypted.

6.6 Users should not share their devices carrying AKU information or data with their family members, friends or third parties.

6.7 Personal devices can only be connected on AKU wireless network using AKU credentials if it is necessary.

6.8 All AKU information or data stored on user's devices should be removed once it is no longer required. This includes documents, spreadsheets, presentations, copies of email attachments, AKU applications and any sensitive information related to AKU.

6.9 Users must remove AKU data and applications by resetting the phone to factory settings at the end of device's life or before passing their devices to a new owner.

6.10 Users must not attempt to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak' or "Root" the device. "Rooted" or "jailbreak" device must not be used for official work.

6.11 AKU, ICT does not accept liability for the maintenance, backup, or loss of data stored on user's personal device. It is the responsibility of the individual owner to backup data to other appropriate backup storage systems.

6.12 AKU reserves the right to refuse access to personally owned devices or software where it considers that there is a security risk to AKU ICT systems and infrastructure.

6.13 Users must report the loss of their devices carrying AKU information or data (including email) to the ICT Service Desk immediately.

6.14 Users must report any security breaches to AKU ICT Service Desk immediately.

6.15 Users must ensure and follow AKU Information Classification & Handling policy ADM-P-003 (information classification & Handling).PDF (aku.edu).

7.0 Unauthorized Use:

7.1 Bypassing traffic to access restricted content.

7.2 Visiting unsafe websites, clicking on unknown links.

7.3 Trying to gain access to unauthorized parts of the network.

7.4 Accessing online trading platforms/personal business using AKU network.

7.5 In case of accidental access to unauthorized confidential data or emails; DO NOT store or disseminate the data and inform the supervisor of the event.

7.6 Using AKU service provider apps on insecure devices (devices on which password protection isn't enabled).

7.7 Taking screenshots of AKU apps or pictures in AKU premises is not allowed except when conducting authorized and approved AKU business.

7.8 Running unauthorized scans on network for searching any material/content.

7.9 Devices may not be used at any time to:

7.9.1. Store or transmit illicit materials.

7.9.2. Store or transmit proprietary information belonging to another company.

7.9.3. Harass others.

7.9.4. Engage in outside business activities etc.

8.0 Disciplinary Actions: Failure to comply with these policies may result in loss of access to some or all of AKU ICT resources and/or loss of access privileges to ICT resources. In addition, violators of these policies may be subject to disciplinary action, up to and including termination.

9.0 Compliance Reference:

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

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

9.3 ISO/IEC 27001:2013 standard, clause A.8.1.3. – Acceptable Use of Assets

10.0 Measures of Compliance: Compliance with this policy will be verified through internal and external audits.

11.0 Reference: This policy satisfies the following requirement of the ISO27001:2013.

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
-	-	A.13.2.1	Information transfer policies and procedure	ISO/IEC 27001:2013

12.0 Related Institutional Documents: N/A

13.0 Annexures: N/A

14.0 Author(s):

Name	Designation
Suneel Kumar Panjwani	Head of Information Security
Saad Ameen	Information Security Specialist
Atif Ali	Information Security Analyst
Samra Sabir	Information Security Analyst

15.0 Key Searchable Terms: Bring your own device policy, personal owned devices, Unauthorized use, BYOD.

16.0 Revision History: This policy is subject to review and revision every two (2) years to ensure its effectiveness and alignment with changing organizational requirements and regulatory obligations.

17.0 Documents Change Record:

Review #	Review Date (dd-mm-yyyy)	Description Of Change	Identification of Change
02	24-05-2024	Reviewed and updated the document in accordance with the latest policy document template.	-