Policy Name	**Electronic/Online Access Guidelines for Students**
Policy Number	**AKU-K/ICT/001**
Approved by	**Academic Council**
Date of Original Approval	**08 Nov 2020**
Date of revisions	
Contact	**Office of the Registrar**

Purpose

The Aga Khan University recognizes the role technology plays in a student's life. In an attempt to ensure, to the extent possible, equitable access to technology for teaching, learning and research, the purpose of this document is to provide a framework for secure and equitable access to technology for academic purposes; guidelines to students for acceptable use of internet, email and other IT facilities available at AKU.

In addition, this policy document includes guidelines for secure use of personal devices; and procedures to purchase a laptop from the University, when available.

Applicability

These guidelines are applicable to all students using devices such as smart phones, tablet computers, laptops and similar equipment, which is personally owned or are the property of the University to store, access, carry, transmit, receive or use AKU information or data, whether at home, on campus or while travelling.

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

Students are required to read this document in conjunction with other relevant University polices, such as the Student Code of Conduct, Student Anti-Harassment Policy & Global Information Security Policy (https://one.aku.edu/PK/it/Documents/KeyDocuments/Policies,%20Procedures,%20Protocols,%20Clinical%20Practice%20Guideline/ADM-P-024%20(Information%20Security%20Policy%20Manual).pdf) that and comply with all these polices now in force or as they come in force in the future.

Guidelines: BYOD (Bring Your Own Device)

As a student at the Aga Khan University, you will need to have access to a device that allows you to engage in online, blended and digital teaching and learning approaches used at AKU. The approaches include accessing your course materials via a Virtual Learning Environment, live-stream lectures, online exams, formative e-assessments, online simulations and a lot more in this ever changing world of technology. AKU provides access to computers on the campus. Students may bring their own devices (e.g. a laptop, smartphone or a tablet/iPad) for study purposes.

Responsible and safe use of devices is the responsibility of everyone accessing the AKU Network. All students bringing their own devices are expected to follow the guidelines included in this document to ensure safe use.

For currently supported devices, please refer to IT Equipment Purchase Catalogue (https://one.aku.edu/PK/it/Documents/Important%20Documents/IT%20Purchase%20Catalogue.pdf).

Obtaining/ Buying a Laptop

The University has the following options for you to obtain a laptop.

1. You may borrow one: Depending on availability, you may request to borrow one from the Library Laptop borrowing services. You will be required to fulfil their requirements.

2. You may purchase one: if you are looking to buy one, and you are experiencing financial difficulty, you may apply for financial assistance to purchase one through the University.

Eligibility to request for financial assistance

1. AKU full time students may apply, whether or not they have availed a scholarship/loan from the University. Students who are on part time programmes may apply. The University would consider their request depending on availability of funds
2. Have no access to a laptop or have access to a laptop that does not meet the minimum requirements as specified by the University.
3. Students in the final year of their study are not eligible to apply. This is not applicable to students in a One Year programme of study at the University.

Guidelines for Users

Students must:

1. Ensure they set and use passwords or pin code on their devices.
2. Ensure a strong password is applied. Please refer to the Password Policy for details (https://one.aku.edu/it/Documents/Policy%20Documents/ADM-P-005%20(Password%20Policy).PDF).
3. Ensure to use licensed software and operating system (e.g. Windows 10), illegal or pirated operating system is strictly prohibited.
4. Ensure the password is not shared with anyone.
5. Ensure that their devices are up to date with latest anti-virus software and security updates.

6. Ensure the device is locked automatically when inactive for more than 5 minutes.
7. Ensure data that contains AKU confidential patient or research information is not stored on personal storage devices. This is against University Policy.
8. Ensure if it is necessary to carry the data on a personal storage device, user must ensure that the device is encrypted.
9. Ensure they do not share their devices carrying AKU information or data with their family members or third parties.
10. Ensure the removal of all AKU related information or data stored on the users device when it is not required. This includes, but is not limited to, documents, spreadsheets, presentations, copies of email attachments and AKU applications.
11. Ensure the removal of all AKU data and applications at the end of the device's life and/or prior to disposal to another person or entity.
12. Ensure the removal of all AKU data and applications at the end of the device's life and/or prior to disposal to another person or entity, from all backup systems or media.
13. Ensure they do not, or enable attempts, to circumvent the device manufacturer's security mechanisms in any way, for example 'jailbreak' or "Root" the device.
14. Ensure they accept the 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. Microsoft OneDrive can be used for data storage and backup.
15. Contact ICT Service Desk immediately if unclear of how to follow the above guidelines.

To ensure safety of the AKU users and the network, the following practices are <u>unauthorized</u> when accessing AKU networks or Systems:

1. Disguising one's identity, the identity of their account or the system(s) they use.
2. Sharing passwords and any other secret authentication information.
3. Using another user's credentials.
4. Impersonating another user or organization.
5. Using the Institution's computers, networks, and internet services for non-academic related purposes such as private financial gain; commercial, advertising, or solicitation purposes.
6. Representing as one's own work any materials obtained on the internet (such as term papers, articles, etc.). Internet sources used in a student's work must be cited by the author, publisher, and website address.
7. 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.
8. Using AKU's Internet number space with their own domain.
9. Accessing another student's, faculty's or staff's computer, device, or data without authorization.
10. Reading, copying, altering or deleting another user's data.
11. 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).
12. Installing, downloading, or distributing "pirated" software.

13. Installing any equipment on AKU's network; installations are restricted to authorized devices/hardware and must be approved by authorized ICT management and performed by authorized AKU ICT personnel.
14. Committing acts that would disrupt or interfere with the legitimate activities of other users.
15. 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).
16. Unauthorized use of or forging of email header information.
17. Creating or forwarding "chain letters," Ponzi or other pyramid schemes of any type.
18. Posting identical or similar non-business-related messages to blogs or large numbers of Usenet newsgroups (newsgroup spam).
19. Attempting to bypass or circumvent AKU's security safeguards.
20. Attempting to degrade the performance of any AKU system.
21. Using AKU's IT 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.
22. Accessing inappropriate and illegal content. Such content shall include, but not be limited to:
    - 22.1 Pornographic and obscene material
    - 22.2 Gambling, gaming, dating sites
    - 22.3 Sites with violent content
    - 22.4 Sites with content focused on sexual interests and activities
    - 22.5 Sites with pirated or peer-to-peer content.
23. Bypassing AKU security controls to access restricted content and/or unauthorized components of the network.
24. Visiting unsafe websites or "clicking on" unknown links.
25. In case of accidental access to unauthorized confidential data or emails, users must immediately inform ICT Service Desk.
26. Storing or disseminating any confidential or sensitive information, emails or data accessed accidently.
27. Running unauthorized scans across the AKU network to discover unauthorized material/content.
28. AKU may contact law enforcement authorities to investigate any matter at its sole discretion without notifying the user.
29. AKU has the right to monitor network traffic and check the information stored on ICT assets that belong to AKU. Users must not have any expectation of privacy with respect to the use of ICT assets that belong to AKU.

For more details on acceptable and prohibited activities, please refer to Acceptable Use of IT Assets policy (https://one.aku.edu/it/Documents/Policy%20Documents/ADM-P-010%20(Acceptable%20Use%20of%20IT%20Assets%20Policy).pdf).

IT Security

Reporting of IT Security Concerns

Security of AKU computers, networks and internet services is a high priority. If you come across any malicious activity on your computer, want to report any instance of policy noncompliance, or need any security related support, please contact ICT Service Desk (Ext: 3434, Email: it.servicedesk@aku.edu) immediately.

Disciplinary Actions

Failure to comply with these policies and guidelines may result in loss of access to some or all of AKU systems and/or loss of access privileges to ICT resources. In addition, violation of these policies may be subject to disciplinary action.