



Avicenna International College

AIC Rules and Protocols
R-103

“Avicenna Internet and Email Usage Policy”

All students, employees, and faculty of Avicenna International College (AIC) will have internet access on college premises and will have a personalized email with AIC specifications. This is a service provided by AIC to facilitate education and academic communication for all concerned parties.

General Rules and Considerations

Students, staff and all users must not:

- try to by-pass the AIC computer security systems,
- use the AIC facilities for illegal activities,
- access, send, receive, print, download, upload or store on their Google Drive, any files, apps, programs or materials which are illegal or in any way offensive, including for the purposes of radicalization,
- exceed their data limit for their Gmail account.

AIC has software and systems that can monitor and record internet usage. AIC reserves the right to inspect any files stored on any of its hardware, or on the “avicenna.hu” Google account, to ensure that this policy is effective. Any abuse of email detected will be reported to the concerned authorities. Any violations of this policy should be reported to AIC and will lead to disciplinary procedures. These may include the closure of online accounts and cancellation of a student’s course with no refund of fees.

AIC will:

- provide free Wi-Fi access for students and staff in the AIC campus,
- provide each student with a Google for Education account,
- encourage students and staff to use Google Chrome and Gmail for their internet usage and emails to benefit from Google’s Safe Search, anti-spam and anti-virus tools,
- provide computer access for students when required.

Please note, however, that whilst AIC will always try to ensure reliable internet access and good protection, it is unable to guarantee the complete security of the IT system and internet access, and cannot be held liable for viruses, hacks or any other security issue encountered using the AIC system, equipment and internet provision. The AIC Wi-Fi network should, therefore, be considered as a public network, and students or staff members choosing to use the system do so at their own risk. AIC reserves the right to close any online accounts it has provided for its staff or students.

Responsibilities Regarding E-Safety

E-Safety means being aware of the dangers associated with the internet, emailing, text messaging and other forms of digital communication or access. All staff and students should abide by the code of conduct below, and any disclosures or concerns should be reported immediately.

Code of Conduct for AIC / E-Safety

Read all the points below carefully and implement them at all times.

All staff and students are expected to:

- use the internet and other forms of communication in a safe, sensible and respectful way,
- only access websites, send messages or access and use other resources that are legal, and will not hurt or upset anybody,
- get permission before using someone else's personal information or photo,
- abide by AIC's internet and email usage policy,
- be aware of, and avoid, the dangers involved in being online, such as:
 - giving out personal details or posting personal images online,
 - sending or receiving an unwanted or upsetting text or email messages or images,

- sending or receiving bullying or upsetting messages or posting malicious information about another person,
- being “groomed” by an adult with a view to meeting the young person for illegal purposes including sex, drugs or crime,
- viewing or receiving socially unacceptable material such as inciting hatred or violence,
- ignoring copyright law such as by downloading music, films or pirated materials.

Acceptable Behaviour in Email Usage Policy

The following explains examples of acceptable behavior while you are using the internet and email provided by AIC.

1. Email users are required to only use AIC email addresses for College purposes or university applications, university admissions and any related educational activities.
2. AIC email accounts are username and password protected. Users are required to be familiar with the AIC's Policy for Passwords, Identity, and Access.
3. Shared, non-personal accounts are approved solely for the handling of AIC business and are the preferred way of managing administrative correspondence within AIC offices and departments.
4. The designated owner of a shared account is the only person entitled to manage the account password. The designated owner may delegate account access rights to any number of other users, but should not disclose the password to them.
5. The use of email must in all ways meet the conditions of AIC's policies concerning communications, equality, diversity, and respect.
6. Email users are individually responsible for managing all their emails properly. This involves, but is not limited to, the following tasks:

- a. Checking and responding to incoming mail appropriately,
 - b. Retaining messages with ongoing academic relevance,
 - c. Ensuring that stored emails can be readily searched, located and retrieved by using meaningful subject lines.
7. Email users are required to avail themselves of appropriate and current protection, such as anti-virus applications, software patches, and updates.
 8. Users must take reasonable measures to prevent the transmission of viruses by not opening attachments received from unsolicited sources.
 9. Email users should always ensure that they send messages only to their intended recipients and clearly flag messages if they are confidential.
 10. Email users who receive any emails with prohibited content from any AIC email address should report the matter to support@avicenna.hu immediately.

Unacceptable Behaviour and Prohibited Content

All AIC email and internet users should be familiar and aware of the material which is legally and naturally prohibited to be included in any email. No such contents should be used and transmitted via the AIC email system.

Below categories of email content prohibited from sending or receiving are shown.

Malicious	Viruses, worms, Trojans, bulk dispatch of unsolicited emails.
Illegal	Pornography, terrorism/extremism, libelous, material over which a third party holds an intellectual property right, forged, anonymous or in any way deceptive email messages or headers.

Offensive	Sexist, racist, harassment, bullying content including offensive comments about hair color, disabilities, age, sexual orientation, religious beliefs and practice, political beliefs, national origin or any other illegal or inappropriate material.
Sensitive personal data	Disciplinary matters, health/medical information.
Commercially sensitive data	Financial information, contractual negotiations, intellectual property.
Other	Support an organization other than AIC; expose AIC to legal liability or reputational damage.

Personal Use of AIC Email

A reasonable level of personal email use is permitted on a conditional basis. It is a privilege, not a right and users must comply with all the rules and regulations of AIC. Personal use must not interfere with AIC business or the performance of specific AIC duties. Email users must ensure that personal messages are not and cannot be interpreted as official communications made on behalf of AIC. Shared accounts are approved solely for the handling of AIC business and personal use is prohibited.

Abuse includes the use of personal email:

- Interferes with any teaching or assessment event or other AIC activity.
- Significantly impedes or adversely affects network performance and or other IT services including file storage capability.
- Causes unwarranted expense, disruption or liability to be incurred by AIC.

Other Conditions and Rules Governing the Use of Avicenna Email

While the privacy of each user mailbox is respected, a number of controls as listed below may apply:

1. AIC reserves the right to monitor and where necessary to suspend accounts to preserve the integrity and operation of the email service.
2. In the event of any breach of network security, AIC reserves the right to force a reset of user passwords across the institution.
3. Emails sent, received or generated in the course of all AIC business, academic and administrative, are the property of AIC.
4. AIC owns the intellectual property rights in all emails generated by its staff in the course of the AIC's business.
5. Email addresses are created and assigned at the discretion of AIC; all addresses have the AIC's core domain name.
6. Email accounts are automatically closed and email addresses canceled whenever a user's formal association with AIC ends or at the discretion of AIC.
7. Email users have a designated email quota. A warning message will be sent when a mailbox reaches near capacity.
8. For practical reasons the maximum size allowed for any single message and attachments within the AIC email system may be fixed and adjusted from time to time.
9. Email users should note that the used anti-spam facilities may result in messages going "missing", as AIC will take steps to prohibit spam.
10. In line with the AIC security policy, email accessed on a mobile device should be protected.
11. Students agree exclusively that they do not change the settings and password of the Avicenna student email and if there is an eligible reason for changing the password, students have to request such change by sending an email and ticket to the computer department.

12. The inbox of any email user may be accessed at any time by IT Services where this is necessary to ensure continuity of or avoid disruption to AIC's business and for other lawful reasons.
- 13. When you register at AIC as a student or staff or faculty, you start the use of AIC email facilities. At this point you have AGREED the "Avicenna Internet and Email Usage Policy" and accepted all the terms and conditions stated in this policy. Breaches of these regulations are subject to AIC disciplinary procedures or further legal actions in the court of justice.**