Ibn Sina National College for Medical Studies
Accredited by NCAAA

كلية ابن سينا الأهلية للعلوم الطبية
معتمدة من
المركز الوطني للتقويم و الاعتماد الأكاديمي

Acceptable Use Policy for the E-mail

Version: V1.0

Overview	This policy defines the acceptable use of the College's email service.
Scope	This policy applies to all employees, academic staff, students and guests of Ibn Sina National College.
Objective	The objective of this policy is to ensure optimum and secure usage of the email service by academic staff, employees, students, and guests.

Policy:

1. Users must use the college's official email services in official business, and should not use free email services such as Yahoo, Gmail and Hotmail.
2. Password sharing is prohibited.
3. Users should not use College email in private transactions.
4. Users are only allowed to send emails and attachments that conform to the religious, cultural, political and moral values of the state. Furthermore, it is not permitted to send messages that may harm the College, ruin its image, or tarnish its reputation.
5. Users are prohibited from participating in publishing emails for personal, commercial, religious or political reasons.
6. Users are prohibited from participating in publishing emails for charitable purposes.
7. Information may be exchanged via email only in accordance with data classification and information processing procedures.

8. Users are allowed to check their email accounts, but are not allowed to upload any College information to their own email account.
9. The following disclaimer must be appended to all emails issued by the College:

> Disclaimer: The information contained in this message is intended for the addressee only and may contain classified information. If you are not the intended recipient of this message, please delete this message immediately and notify the sender; you should not copy or distribute this message or disclose its contents to anyone. Any views or opinions expressed in this message are those of the individual(s) and not necessarily of the college. No reliance may be placed on this message without written confirmation from an authorized representative of its contents. No guarantee is implied that this message or any attachment is virus free or has not been intercepted and amended.

Executive Policies and Procedure:

1. Users shall use email forwarding with due care, and should not forward junk, spam, or marketing emails.
2. Users are not permitted to send, reply or forward emails containing confidential information, or are considered to contain material that breaches intellectual property rights.
3. Users are prohibited from sending, replying, or forwarding emails that contain attachments that are infected with viruses or any malicious software.
4. Users should not open spam emails, and they should delete them from the system.
5. Users are prohibited from using the College email system to impersonate someone else.
6. Users are prohibited from sending, forwarding, transferring, distributing or replying to emails when using someone else's email system.
7. Users are prohibited from entering any changes to the content, date, time, source, people, addresses, or other information in the email.
8. Users must check and ensure that email attachments are virus-free and do not contain any malicious code.
9. Users must use signatures and disclaimers approved at the College, with all emails.
10. Users should not register or share their email address on websites for purposes not related to work.
11. Users should not use the automatic forwarding feature to or from external email addresses.
12. When using an email on a mobile phone such as smart phones, you must provide the mobile phone with the feature of an automatic security lock and password when you are not using the phone.

Attachment Opening Policy:

1. The e-mail must be from a known sender and make sure that his e-mail is correct and not the e-mail of another person who impersonates him and is from outside the organization.

2. When ensuring the safety of the sender and making sure that he knows that his mail is not for someone impersonating his identity, download the attachment only, and then go to a file-checking site such as VirusDesk Kaspersky.

3. If the result of the file analysis is safe, and the file contains links that must be checked before clicking on them by copying and checking them through link checking sites such as VirusTotal.