

Iqra University Email Policy

1. Introduction

This document serves as the University's policy on email, as well as appropriate procedures and guidelines for their use. Communication using emails is one of the important and official ways of communication, therefore the University's policy on email and offering appropriate procedures on the use of this facility is necessary.

Email services are provided by the University to support its core functions related to academics, research and associated management.

The purpose of this policy is to ensure the proper use of the IQRA University email system. It aims to ensure secure and responsible email practices, maintain data integrity, and comply with relevant regulations.

2. Purpose

The purpose of this policy is to:

- Improve the successful delivery of university communications to all faculty, staff and students.
- Email is used by the University community in an ethical and considerate manner in compliance with applicable laws and policies.
- Reduce the risk of university data classified as Legally Restricted or Confidential going through email systems that are not managed by the University.
- Email users are informed about how concepts of privacy and security apply to email, as well as the applicability of relevant policies.

3. Scope

This policy applies to all email accounts issued by the University and is intended for IU domain-based email i.e., alias@iqra.edu.pk accounts only for faculty, staff, students, and aliases.

4. Responsibilities

- **University IT Department:**
 - Manages the University email system and ensures its security.
 - Provides support to users regarding email accounts and functionalities.
 - Monitors email activity for suspicious behaviour.
- **Email Users:**
 - Comply with the terms of this policy.

- Maintain the security of their email accounts by using strong passwords and avoiding suspicious links or attachments.
- Report any suspicious email activity to the IT Department.
- **Department Heads/Managers:**
 - Ensure their staff are aware of this policy and its implications.
 - Address any violations of this policy within their departments.

5. Acceptable Use

University email accounts are intended for official University business purposes, including communication, collaboration, and information sharing.

6. Unacceptable Use

The unacceptable use of email is considered a serious breach of the code of conduct and may result in action taken under the Academic Regulations, IU Statutes for students and HR Manual “Code of Conduct” for faculty and staff.

It is not possible to make an absolute definition of inappropriate and unacceptable use; however, the following sub-sections of this policy outline possible instances that are deemed unacceptable or inappropriate

- a. Any use of a commercial or profit-making nature, or for any other form of personal financial gain.
- b. Any use of those conflicts with an employee's obligations to the IU.
- c. Use considered to be against the IU rules, regulations, policies and procedures of the Email Use Policy.
- d. Transmission of large files (documents or software) for personal use.
- e. Introducing or attempting to introduce computer viruses by email messages or attachments
- f. Creation or transmission of material that is defamatory or material that includes claims of a deceptive nature
- g. Creation or transmission of material that is abusive or threatening to others serves to harass others or is designed to cause distress, inconvenience or anxiety. For example, material that discriminates or encourages discrimination on the grounds of Race or Ethnicity, Gender, Sexual Orientation, Marital Status, Disability, Political or Religious Beliefs. Similarly, the creation or transmission of any offensive, obscene or indecent images, messages, data or other material will be considered unacceptable.
- h. Creation or cascading of emails using IU-provided email services containing material that brings the IU into disrepute.
- i. Creation or cascading of emails using IU-provided email services containing unsolicited commercial or advertising material

- j. Creation or cascading of chain letters or junk mail of any kind
- k. Creation or cascade of anonymous messages or deliberately forged messages
- l. Use of IU-provided email for activities that violate the privacy of others or unfairly criticise and misrepresent other individuals
- m. Use of IU-provided email for activities that corrupt or destroy other users' data or disrupt the work of other users
- n. Routing external communications in a manner that deliberately attempts to bypass any system logging or audit functionality
- o. Users disguising himself or herself or their sending addresses when they use the service in order to misrepresent any aspect of a communication.

In addition, users should be aware of their responsibilities to;

- a. Ensure that the identity of the recipient to whom they are sending an email is correct.
- b. Reasonably understand copyright, trademark, libel, slander and public speech, so that their use of the email service does not inadvertently violate any laws which might be enforceable against the IU.
- c. Check before forwarding any emails received from others as these may contain confidential or sensitive information, which should not be shared.
- d. Also consider and adhere to general guidelines as laid down in Ch of “IU Students Handbook” for students.

7. Password Management

Users are responsible for maintaining the security of their email accounts by using strong passwords. Strong passwords should:

- Be at least 12 characters long.
- Include a combination of uppercase and lowercase letters, numbers, and symbols.
- Not be easily guessable (e.g., birthdays, pet names).
- Be changed regularly (at least every three months).

Users must not share their passwords with anyone.

8. Email Retention

IU emails remain activated as long as the user account is officially active. Staff / Faculty Emails shall be deactivated after the employee resigns or is terminated from his/her services.

NOTE: Students' email IDs are deactivated/deleted after the completion of the degree program.

9. Email Accounts

- **Creation:**
 - Email accounts are created for authorized users by the designated department (e.g., HR for staff, Student Service Center for students).
 - The naming convention for email accounts will follow a standardized format.
- **Deletion/Deactivation:**
 - If the email account is involved in any SPAM activity results in email server choking. IT Manager/Network Administrator will delete or disable email accounts.
 - If a deletion request is received from the email owner.
 - Users have a limited grace period to back up their data before account deletion.
 - In case of Resignation, Termination or retirement of an employee, the email accounts will be deactivated. However, 3-day duration will be provided for backup purposes from the last working day of an employee.

10. Email Signatures

All email users are encouraged to create a professional email signature that includes the following information:

- Name
- Job Title
- Department
- Location/Address
- Telephone Number and Work Mobile
- University Website URL

A standardised disclaimer regarding confidentiality and legal restrictions will be automatically added by the University email server. In addition to the individual signatures, the following will be the institutional disclaimer added by the IU email server for each email:

Employee Name

Designation

Campus Address

Campus UAN: +92 21 111-264-264 Ext XXXX

email address@iqra.edu.pk

www.iqra.edu.pk

Disclaimer: The message contains information which may be confidential and privileged. Unless you are the intended addressee or authorized recipient of the addressee, any distribution, copying or disclosure of the message or any information obtained from the message is strictly prohibited. If you have received this message in error, please notify the sender and then delete the message from

your system. We appreciate your understanding.

11. Spam & Phishing

All incoming emails are scanned for viruses, phishing attacks and SPAM. Suspected messages are blocked from the user's inbox. Due to the complex nature of email, it is impossible to guarantee protection against all SPAM and virus-infected messages. It is therefore incumbent on each individual to use proper care and consideration to prevent the spread of viruses. In many cases, viruses or phishing appear to be sent from a friend, coworker, or other legitimate source. Do not click links or open attachments unless the user is sure of the nature of the message. If any doubt exists, the user should contact IT Helpdesk and Support Services.

12. Email Storage

Storage Limits:

- HoDs and above: 25GB
- Staff : 10 GB
- Faculty : 10 GB
- Visiting Faculty: 5 GB
- Students : 5 GB

13. Value Addition

In addition to email storage, 1TB of Microsoft OneDrive cloud storage shall also be available to all registered email users. Email Users shall also be allowed to freely download Microsoft Office 365.

14. Incident Management

Users are required to report any suspicious email activity, such as phishing attempts, to the IT Department for investigation.

15. Access Control

The University implements access controls to restrict unauthorized access to email accounts.

16. Change Management

The University follows a change management process for any modifications to the email system or this policy to minimize disruption to users.

17. Review

This policy will be reviewed periodically and updated as needed to reflect changes in technology, regulations, or University procedures.

18. Breaches of Policy

Violations of this policy may result in disciplinary action, up to and including termination of employment or expulsion from the University.

19. IT Support Services

All communication related to the creation of email accounts and support be directed to the following:

-

S. No	Campus	Extension	Email Address
1	Main	9851, 9852	helpdesk@iqra.edu.pk
2	Gulshan	4802,4803,4804	helpdesk.iugc@iqra.edu.pk
3	North	1803,1806,1810	helpdesk.iunc@iqra.edu.pk
4	Airport	5802,5803	helpdesk.iuac@iqra.edu.pk
5	Bahria	8500	helpdesk.iubc@iqra.edu.pk