Alfaisal University

Policy Name:	Email Usage Policy

Version #	**01**
Date Approved	
Effective Date	
Policy Owner	IT Services

Summary:

The University's email system can be used to distribute information by a specific user (i.e. students, faculty and staff). Email messages to specific secure groups require authorization and approval by the executives as specified in this document.

Signature: ……..

Table of Contents

1. Introduction 3
2. Purpose 3
3. Policy Scope 3
4. Policy for Acceptable Use of Emails 3
4.1. Acceptable Use of Emails Statements 3
4.1.1. Users should refrain from using Alfaisal email ID for personal emails. 3
4.2. Acceptable Use of Emails Guidelines 3
4.3. Email Broadcasting 3
4.4. General Email Broadcasting Statements 4
4.5. Email Broadcasting Guidelines 4
4.6. Email Safety and Spam Control 5
4.7. General Email Safety and Spam Control Statements 5
4.8. Email Safety and Spam Control Guidelines 5
6. Mailbox Statements 6
6.2. Mailbox maintenance email archiving and storage 6
6.3. Mailbox guidelines 6
7. Email Account Policy for Employees Leaving Alfaisal 7
8. Exemptions 7
9. Enforcement 7
10. Definitions 7

1. Introduction

The University's email system can be used to distribute information by a specific user (i.e. faculty, staff and students). Email messages to specific secure groups require authorization and approval by the executives as specified in this document.

2. Purpose

This document describes Alfaisal policy regarding the email usage. Which covers acceptable use of emails, broadcasting, email safety, archiving and storage capacity of the mailboxes. Effective use of this policy depends on the University's ability to use it prudently

3. Policy Scope

Access to the University's email service is limited to Alfaisal employees and students or individuals who have been designated to perform this function by The president office ,the Provost, VPs, Deans, Department Heads or the IT Director.

4. Policy for Acceptable Use of Emails

4.1. Acceptable Use of Emails Statements

4.1.1. Users should refrain from using Alfaisal email ID for personal emails.

4.1.2. Passwords should not be shared with anyone and should not be sent through emails.

4.1.3. Alfaisal internal announcements/emails or mails containing sensitive information should not be forwarded or transmitted in any form to anyone outside Alfaisal.

4.1.4. Users should not subscribe or participate in any email list using their Alfaisal email ID that provides access to unsuitable content.

4.1.5. Users should not mail or forward obscene, disrespectful, or offensive material.

4.1.6. Use of offensive, abusive, violent, threatening and harmful content through emails is strictly prohibited.

4.1.7. Alfaisal reserves the right to track, access, block, drop or redirect mails which could damage the harmony and integrity of Alfaisal.

4.2. Acceptable Use of Emails Guidelines

4.2.1. If a user receives an email containing offensive, obscene, or improper content, he should immediately inform the ITS (IT Services).

4.2.2. Users should immediately inform any identity theft or spoofing to the ITS.

4.3. Email Broadcasting

Email Broadcasting is meant to reach specific audience in order to convey important,

relevant information. Alfaisal email broadcasting system is for the delivery of important, emergency or time-sensitive information. Messages which must be communicated quickly should use multiple methods of conveyance.

4.4. General Email Broadcasting Statements

4.4.1. The message must be from a valid alfaisal.edu email account

4.4.2. ITS will create and maintain secure/unsecure groups for targeted university audiences.

4.4.3. Designated personnel are only authorized to send broadcast messages to specific secure group(s).

4.4.4. All broadcasting messages should have a short and clear descriptive subject for the message.

4.4.5. The use of attachments should be minimal for all bulk broadcasting messages.

4.4.6. It is the responsibility of the department to determine the appropriateness of the messages, proofreading, and following the guidelines for sending broadcast messages.

4.4.7. The message must concern Alfaisal, and it must be sponsored by a department.

4.4.8. The broadcast subject should be sent by only one person and not be redirected from another.

4.4.9. The email subject should reflect the Topic/Agenda/Event that is scheduled to occur.

4.4.10. A signature is required from department personnel that contain a phone number.

4.4.11. All html links if provided must be functional and from a valid source

4.4.12. Broadcast messages must be sent at least one business day prior to the event or program being publicized.

4.4.13. Messages concerning personal events, business or promotional in nature should not be broadcasted.

4.4.14. This provision explicitly prohibits the posting of unsolicited electronic mail to lists of individuals, and the inclusion on electronic mail lists of individuals who have not requested membership on the lists.

4.4.15. Student's electronic mailing list for a class in which they are registered would be used for the purpose of official communications between authorized University personnel and an identified group of students.

4.5. Email Broadcasting Guidelines

4.5.1. Check the email twice before sending.

4.5.2. Know your intended group or audience.

4.5.3. User should consult ITS or refer the Policy Based Distribution Groups Document for the Distribution Groups available in the email system.

4.5.4. Broadcast email messages are not recommended as the only means of communication for circulating emergency or particularly time-sensitive information.

4.5.5. Keep it simple. Brief, plain text messages are advised not to use graphics, embedded images or attachments instead can use links to direct recipients to a portal / website where they can obtain more information

4.5.6. Use resources wisely. Email is a university resource which should be used sensibly.

4.6. Email Safety and Spam Control

Email protection is “enabled” on the email Server to provide defense against malicious infections such as Spam, virus, Trojans, worms, spoofing and other malware. Users may not purposely send or forward emails containing viruses or other malicious infections.

4.7. General Email Safety and Spam Control Statements

4.7.1. If the user receives any infected email, immediately notify ITS to take proper action.

4.7.2. Spam Filtering is enabled on the email Server based on a spam score as determined by the global standard.

4.7.3. Spam mail(s) will be either quarantined or redirected to the Junk folder of the recipient.

4.7.4. Emails that are identified by the scanner as infected will be automatically quarantined.

4.7.5. Quarantined emails will be kept for 7 days; after which they will be automatically deleted.

4.7.6. The user is responsible for checking the Junk folder regularly to ensure that spam emails have been categorized correctly.

4.7.7. If a genuine email is categorized as Junk, the user should set it to "non-spam" as specified within the email in order to receive it in inbox i.e.to the safe list.

4.8. Email Safety and Spam Control Guidelines

4.8.1. If the user receives a message from an anonymous source, or strange subject line, he should inform ITS and delete that email immediately.

4.8.2. The user should not reply to emails from unknown senders.

4.8.3. Users should avoid using their Alfaisal email address in chat rooms, newsgroups, and mailing lists. The chances of receiving spam emails increase when an email is publicly posted.

4.8.4. Users should consider using filtering on incoming mail in their email client (Microsoft Outlook).

4.8.5. Emails identified as spam will be automatically received into the junk folder. Users are advised to regularly check the junk folder to identify any emails that

were mistakenly categorized as junk by the email system.

6. Mailbox Statements

6.2. Mailbox maintenance email archiving and storage

6.2.1. Alfaisal ITS offers email accounts in Outlook, and Webmail access. Users are responsible for setting the mailboxes on their personal smart devices.

6.2.2. ITS provides the default configuration in Microsoft Outlook. Users are responsible for setting personalized mail features such as signatures, out of office replies that are in line with Alfaisal standards.

6.2.3. Users are responsible for keeping their email account's size under the assigned quota threshold by deleting unnecessary emails and/or archiving old emails by storing them locally. ITS will provide required assistance.

6.2.4. Whenever mailbox reaches 90% of its allocated size, the user will be automatically warned to clear up space from his email account. When the account reaches 100% the user will automatically receive an email notification and will not be able to receive new mails. In order to receive/send new emails again, the user should clear up space in his account by deleting unwanted emails, archiving old emails, deleting emails with big attachments, etc. For assistance on how to clear and archive emails, users can contact the ITS.

6.2.5. Spam emails will be received in the junk folder which also adds up to the mailbox quota.

6.2.6. Email accounts are backed up regularly on a daily, weekly, and monthly basis.

6.3. Mailbox guidelines

In order to have a safe and secure network environment, all users at Alfaisal must adopt the following precautions:

6.3.1. Webmail is enabled to provide access to email through http://webmail.alfaisal.edu for Employees and http://smail.alfaisal.edu for Students .

6.3.2. Whenever users access their webmail from a public PC, they should make sure to log off (Sign off) their Alfaisal email account before ending their session.

6.3.3. Should a user require delegating access rights to view or send an email on his/her behalf, these rights should be granted very cautiously and to very few. The user however, will be held responsible for emails generated and sent from his account.

6.3.4. Forward suspected hoax messages to itsupport@alfaisal.edu

7. Email Account Policy for Employees Leaving Alfaisal

7.2.1. Alfaisal email account will be deactivated after ITS signing off the clearance form.

7.2.2. Employees leaving Alfaisal for good should relinquish the privilege of sending emails to secure distribution groups. HR should instruct IT Services about such matters.

8. Exemptions

Exception to or exemptions deviating from any provision of this policy must be approved by the VP for Finance & Administration or the President. Similarly, any questions about the contents of this policy, or the applicability of this policy to a particular situation should be referred to the IT Director.

9. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action as per the University code of conduct.

10. Definitions

Alfaisal User	Any computer user with user identification that have access to Alfaisal(s) computer facilities in or off campus. This covers permanent and temporary Faculties, Staff, Visitors, Guests, Contractors, Vendors, or any Third parties.
Distribution Groups	Is a term sometimes used for a function of email clients where lists of email addresses are used to email everyone on the list at once
Spam	Unsolicited or undesired electronic messages
E-mail spoofing	Is a term used to describe (usually fraudulent) e-mail activity in which the sender address and other parts of the e-mail header are altered to appear as though the e-mail originated from a different source. E-mail spoofing is a technique commonly used for spam e-mail and phishing to hide the origin of an e-mail message