جامعة اليمامة
Al Yamamah University

YU Policy on Effective Use of IT Resources

Policy Owner	University Council
Policy Author	IT Department
Version	V 1.0
Issuing Authority	University President
Document Date	20th February 2023
Circulation	All Faculty, All Staff, All Students
Effective Date	27th February 2023
History	The policy is prepared by IT Department. Reviewed and Approved by the University Council in its meeting on 20th February 2023.

DCO Form V1.1

YU Policy on Effective Use of IT Resources

Contents

Introduction 3

Purpose 3

General Guidelines and Procedures 3

Ethical Guidelines: 3

Allowed Use of Equipment 4

Prohibited Use: 4

Accountability 4

E-mails 4

1- University Property 4

2- Inappropriate E-mails 5

3- Confidentiality and Security 5

4- Representing the University 5

5- Disclaimer: 6

6- External Files and Attachments 6

7- Phishing and Scam 6

Accessing YU Computer Laboratories Facilities: 6

Scope 7

Exception 7

Authorization 7

Introduction

The Information Technology (IT) Department at YU oversees all tasks related to the effective and ethical use of IT within the YU community, including tools, equipment, computing resources, and IT laboratories. The IT department is responsible for ensuring that YU community is following the best practices and following code of conduct TYU staff is also involved in providing guidance to YU community on how to follow this code of conduct.

Purpose

This policy describes the procedures implemented by the IT Department to make sure that all tools, equipment, computing resources, and IT laboratories at YU are used in a professional and ethical manner by YU students and faculty.

General Guidelines and Procedures

- The YU community is to conduct themselves professionally in matter that upholds the reputation and ethics of the university.
- All users are issued with a unique username and password. The person assigned their username and password is solely accountable for all actions performed under their username and password.
- YU IT Department is responsible for ensuring that the university's computing, networking, and telephony resources are properly used and protected by maintaining the integrity, security, and privacy of the resources and of users' electronic files, mails, records, and activities.
- Security measures are put in place to assist with investigations of illegal and criminal activities or policy violations.
- Downloading and installing software must be done only in coordination with the IT Department.

Ethical Guidelines:

1. Respect the intended use of all IT resources for learning, teaching, research, and university business purposes.
2. Respect other users by not sending unwanted e-mail messages, mailing address information, flooding the system, sending frivolous messages, forging subscriptions, or tampering with accounts, files, or data that are not owned by your account.
3. Be sensitive to the public nature of shared resources, i.e. labs, internet usage, and disk space.
4. Occasional unsolicited receipt of e-mail should be avoided. Report repeated unsolicited receipt of e-mails to IT department.
5. Report misuse of Information Technology resources. Complaints regarding misuse of IT resources should be reported to the IT Department immediately.

Allowed Use of Equipment

IT resources should only be used for activities that support YU mission of the university: learning, teaching, research, and university business.

- YU may, as a matter of discretion, allow the use of university systems for other purposes including personal use, so long as this:
  1. Does not interfere with other codes of conduct.
  2. Does not affect work duties.
- Excessive use of the telephone, e-mail, Internet facilities or computer systems for personal business may result in a disciplinary action.
- YU may cease to allow such other uses at any time.

Prohibited Use:

University Systems must not be used to:

1. Send or receive material that is, or may be construed to be, obscene, derogatory, defamatory, harassing, threatening, vilifying, racist, sexist, sexually explicit, or otherwise offensive or excessively personal.
2. Send or receive material which harasses or promotes hatred or discrimination based on any unlawful grounds against any person (refer to the university's anti-discrimination Policy).
3. Harm the reputation of the university or cause embarrassment to the university.
4. Send or receive material relating to the manufacture, use, sale or purchase of illegal drugs or dangerous materials or to any other illegal activity.
5. Spam, mass mail, or send or receive chain mail.
6. Infringe the copyright or other intellectual property rights of another person.
7. Perform any activity using an anonymous or misleading identity.
8. Engage in any other illegal or inappropriate activity.
9. Provide services or produce materials for commercial gain, or access some social networking sites including, but not limited to, Facebook, Twitter, Instagram,... etc.

Accountability

Any university employee may be held responsible for any:

1. Damage to the university's equipment caused by their misuse of university systems.
2. Costs incurred by their access to prohibited Internet sites.
3. When using the Internet and electronic communications, YU employees must:
   a. Always identify themselves clearly and honestly.
   b. Not share their passwords or credentials except as required by the university.
   c. Never access another person's email or system account without that person's permission.

E-mails

1- University Property

YU is the owner of copyright over all e-mail messages created by its employees as part of their employment. The university may keep copies of employees' mailboxes for later references.

2- Inappropriate E-mails

- The employee and/or the university will be liable for what is written in an e-mail message.
- If you receive an e-mail which you think may be a sort of scam or trying to impersonate someone, it must be forwarded to the IT Department.
- Avoid the use of overly expressive punctuation and text formatting that can be construed in a negative way: exclamation marks, capitals, underlining, and font size are all examples that can be received negatively if used inappropriately.
- Sarcasm is also often misconstrued in emails and should be avoided. A phone call or face-to-face meeting is often the best form of communication.
- If you receive an e-mail which you think may be inappropriate from any member of YU community, do not respond to it. Please write an official complaint to your direct supervisor (for employees) or department chair (for students) and attach the email with your complaint.

3- Confidentiality and Security

- When an e-mail is sent from the university to the network server/ cloud-based service and then on to the Internet, the e-mail message may become public information.
- E-mail messages which contain sensitive information should be encrypted before sending.
- Items of a highly confidential or sensitive nature should not be sent via e-mail, even with encryption. On occasion, e-mails may be used to correspond with recipients who are unknown or cannot be identified.
- The intended recipient should be identified prior to sending or receiving an email, and care should be taken when sending or responding to such e-mail messages. There is also a risk of false attribution of e-mails.
- Some software are widely available by which e-mail messages may be edited to reflect an erroneous message or sender name. The recipient may therefore be unaware that they are communicating with an impostor. Accordingly, you should maintain a reasonable degree of caution regarding the identity of the sender by other means if you have concerns.
- E-mails may be truncated, scrambled, delayed, sent to the wrong address, or not arrive at all. If an outgoing email is important or urgent, you should verify that the recipient has received that e-mail in its entirety.

4- Representing the University

When sending e-mail messages for the university's business purposes, YU employees must ensure that:

- Any representations made are those of the university.

- The manner of expression used in that e-mail is consistent with the relevant business purpose.
- Comments that are inappropriate in the workplace is also considered inappropriate when sent by e-mail. As noted above, e-mail messages can easily be misconstrued.
- Words and attached documents should be carefully chosen and expressed in a clear and professional manner.

5- Disclaimer:

You must ensure that all messages that are sent from your e-mail address contain the university's standard disclaimer message, which reads as follows:

This message and all of its contents and attachments are confidential and may contain legally privileged information for Al Yamamah University. Please delete this message with all of its content if you are not the intended recipient. You should not copy this message or distribute its contents to anyone. Statements and opinions expressed in this e-mail are those of the sender, and do not necessarily reflect those of Al Yamamah University.

6- External Files and Attachments

All external files and attachments must be virus checked using an installed scanning software before they are accessed. Virus checking is done automatically through the software installed on the mail server. If you are concerned about an e-mail attachment or believe that it has not been automatically scanned for viruses, you should contact the IT Department.

7- Phishing and Scam

- To avoid phishing tricks, YU users should avoid clicking on links received by email, especially if received from unknown or a doubtful person, and they must not enter their credentials. It is important to check that accessed website is the intended one and not a misleading copy.
- Employees who receive emails that appear to come from their administrative superior and request them to buy or pay some expenses urgently should report this request to the IT Department as these requests are most likely coming from impostors.

Accessing YU Computer Laboratories Facilities:

- Computer labs are only accessible for authorized faculty members who are assigned classes in that laboratory facility, so all computer laboratories in YU are locked by access control systems using the fingerprint access to avoid unauthorized access to the computer laboratory and ensure an effective use of those laboratories.

- Faculty members who have scheduled classes of a specified laboratory facility should share their schedule with the IT Department in order to provide a fingerprint access to that particular laboratory facility.
- Anyone who does not have a permission to access the computer laboratory facility is not allowed to access that laboratory.

Scope

This policy applies to the effective use of all IT services, tools, equipment, computing resources, and computer laboratories used by all academic programs in different departments and colleges that might be presented in different administrative and services units of YU.

Exception

The University-Council reserves the right to make alternative decisions based on any situation or circumstances outside the conditions stated in this policy.

Authorization

The policy was authorized and made effective by the university president.

University president	**Date**
	28-2-2023