It's your future too

POL/IT/0039: Email Policy

Policy Title:	GEMS Education MENASA ICT – Email Policy
Policy Number:	POL/IT/0039
Version:	1.0
Effective date:	29 September 2022
Scheduled review date:	28 September 2024
Policy approver:	Chief Disruption Officer
Policy owner:	SSC IT
Policy reviewer:	IT Heads of Department
Relevant related policies:	• Refer Section 6
Other relevant documents:	• None

Table of Contents

1. Policy Statement

Electronic email is the primary communication method within GEMS. Misuse of email can post many legal, privacy and security risks, thus it is important for users to understand the appropriate use of electronic email communication.

2. Purpose

The purpose of this email policy is to ensure the proper use of GEMS email system and make users aware of what GEMS deems as acceptable and unacceptable use of its email system. This policy outlines the minimum requirements for use of email within GEMS or Non-GEMS Network.

3. Scope

This policy applies to all individuals working at all levels and grades, including all teaching staff, senior managers, officers, directors, employees (whether permanent, fixed-term or temporary), consultants, contractors, seconded staff, casual workers and agency staff, of GEMS, wherever located.

4. Requirements

GEMS personnel should use their business email account with due care to avoid misuse.

4.1 GEMS personnel shall not:

- Use GEMS email account for any personal communication and will only be used for GEMS business related purposes;
- Use GEMS business email address to subscribe to mailing lists, external services not related to business;
- Utilize named GEMS email accounts (allocated corporate email accounts) for promotional messages or advertisements;
- Generate or forward chain mails containing derogatory, libellous or threatening messages, images against an individual, race, religion, organization or community;
- Share executable programs or scripts to internal or external recipients over email;
- Remove or modify the system generated disclaimer notice and email signatures;
- Auto-forward GEMS corporate emails to external addresses / domains or personal accounts;
- Utilize alternate modes to communicate GEMS business information such as messenger services or email services not provisioned by GEMS;

4.2 GEMS personnel are not permitted to utilize corporate email for personal correspondence or sending emails to non-GEMS email systems and storage servers such as Google, Yahoo, and MSN Hotmail etc.

4.3 All GEMS data contained within an email message or an attachment must be secured according to the GEMS Data classification policy.

4.4 Under no circumstances should the GEMS mail system be used in a manner to harass or intimidate anyone or for other illicit or illegal purposes. Employees may not use the GEMS mail system to transmit, download, or distribute any confidential company information, threatening materials, obscene materials, or anything constituting or encouraging the violation of any laws.

4.5 Users will not use GEMS email to infringe the copyright or other intellectual property rights of others.

4.6 Email system will not be used under any circumstances to communicate any business-related information to unauthorized recipients.

4.7 GEMS email system will not be used for personal commercial gains such as lottery, advertisements (property, sale etc.), engage in or obtain information for gambling transactions.

4.8 Sending chain letters or joke emails from or to a GEMS email account is prohibited.

4.9 Email Spoofing i.e., constructing an email such that it appears to have come from someone else, is prohibited.

4.10 Users must immediately report to Information Security team for all actual or suspected Information security incidents, or if a Computing Device is lost or stolen.

4.11 Only Computing Systems that have been authorized by GEMS IT must be used to store GEMS emails.

4.12 Users must not reveal their personal information such as passwords, passport, pen card, bank account, credit card details or click on any hyperlinks embedded in an email that appears to have come from a valid source to avoid phishing attacks. These messages must be immediately reported to Information Security Team.

4.13 GEMS personnel shall exercise caution in responding to requests soliciting user credentials for GEMS accounts that claim to come from ICT department or service providers over email or telephone calls;

Note: Under any circumstances, GEMS ICT or any service provider will not request validation of GEMS user accounts or user credentials (username / password) over an email, URL, SMS or a telephone call. All such requests should be promptly notified to ICT helpdesk and should not be complied with.

4.14 GEMS Education reserves the right to monitor and disclose GEMS provisioned email communications for legal purposes without prior notice. All email correspondence performed using

GEMS corporate email accounts shall remain the property of GEMS Education and is considered official data.

5 Policy Compliance

5.1 Compliance - Information security and IT team shall be responsible to monitor compliance with this policy.

5.2 Exceptions:

- Exceptions to this policy shall be documented and recorded in service desk portal. Exception shall include:
  - Clear Business Justification,
  - Impact / risk resulting
- Exceptional approval process will be initiated once a request from Heads of Department with business justification is received by information security team either by service desk request or by an email.
- Technology Steering Committee will be used to decide on the final decision in case of an escalation.

6 Related Standards, Policies and Processes

- Information Security Policy;
- Acceptable Use Policy
- Security incident Management Policy
- Data Classification Policy

It's your future too

GEMS EDUCATION

7 Appendix – I (Exceptions Form)

Form# Entity-Location/ Department-FOR-EX0001	Date: DD/MM/YYYY
To be filled by Requester	
School:	
Department:	
Employee Name:	
E-mail ID:	
Employee ID:	
Designation:	
Contact Number:	
Exception	
Description	
Risk	
Assets/ policy Impacted	
Ownership of generic ID (if applicable)	
Justification	
Impact:	□Critical □ High □ Medium □ Low
Approval	
Department Head:	
Employee Name and Designation:	
Employee ID:	
Approval Date:	
Status:	□Approved □Rejected
Approval 1	
Employee Name and Designation:	
Employee ID:	
Approval Date:	
Status:	□Approved □Rejected