POL/IT/0018: Acceptable Use Policy

Policy Title:	Acceptable Use Policy
Policy Number:	POL/IT/0018
Version:	1.0
Effective Date:	01 September 2022
Scheduled Review Date:	31 August 2024
Policy Approver:	Chief Disruption Officer
Policy Owner:	SSC IT
Policy Reviewer:	IT Heads of Department
Relevant Related Policies:	N/A
Other Relevant Documents:	N/A

1. Central Policy Statement

This policy provides a governing framework for secure and responsible use of GEMS Education provided computing devices, services and devices connected to GEMS Education networks.

It is the responsibility of every GEMS personnel, to familiarize with this policy and to conduct their activities in accordance with its recommendations.

2. Policy Scope

This policy applies to GEMS MENASA Holdings Limited (the "**Company**" or **GEMS**) who are granted access to GEMS data[1] or its systems, or network which includes:

- All individuals working at all levels and grades, including 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; and
- All of those who represent GEMS Education in any capacity, including agents, sponsors, intermediaries, representatives and finders and introducers.

Throughout this document, all applicable parties have been collectively referred to as "GEMS Personnel".

3. Legal Background

- N/A

4. Underlying Policy Statements

4.1 Ownership and Return of Computing Devices

4.1.1 GEMS Education provides computing devices to its staff and authorized contractors, to support educational and work-related activities. GEMS provided devices shall continue to be the property of GEMS education, unless explicitly documented at the time of allocation;

4.1.2 Upon completion of employment or the contractual term, personnel shall return all computing devices in their custody to the ICT department. Project or department managers shall be responsible to ensure all computing devices issued to third-party

contractors under their care, are returned to ICT department prior to release of contractor personnel.
NOTE: Return of all GEMS provided devices has to be completed to obtain an exit signoff from the ICT department.

4.2 Protection of GEMS issued Computing Device

4.2.1 GEMS Personnel shall adopt reasonable measures to safeguard GEMS issued equipment in their possession from theft and damage:

- Computing devices shall not be left unattended in meeting rooms or at thirdparty locations including conferences or hotel rooms;
- Computing devices shall not be checked-in as baggage during travel, unless mandated by the airport security personnel;

4.2.2 GEMS personnel are not authorized to perform self-repairs. Faulty devices shall be handed over to the respective ICT helpdesk for repairs and maintenance through authorized service vendors;

4.2.3 Incidents related to lost, stolen or damaged computing devices shall be promptly reported to the ICT helpdesk; *NOTE:*

- *On stolen / lost devices End-User is required to obtain a Police report (First Information Report / FIR) from the nearest police station.*
- *GEMS ICT reserves the right to secure erase lost or stolen devices.*

4.2.4 Computing devices including portable storage devices, containing GEMS business information shall be handed over to ICT helpdesk for disposal in a secure approved manner.

4.3 Acceptable Use of Computing Devices

4.3.1 GEMS issued computing devices shall be utilized in a manner that is consistent with organizational policies and within the confines of country laws and regulations. GEMS personnel shall not:

- Bypass organizational or national security measures through fraudulent use of network protocol address i.e., use of private Virtual Private Networks or anonymity networks;
  NOTE: GEMS personnel are only permitted use of corporate Virtual Private Networks to connect to GEMS corporate network from remote locations.
- Download, transmit, store or create inappropriate material that violates organisation policies or laws of the country;
- Perform activities that would cause the network, website or applications to stop functioning or result in crashing, deletion, omission, destruction or cause fraudulent transaction i.e., activities classified as hacking or cracking;

- Install applications licensed as "free for non-commercial use", shareware, adware and those not authorized and not licensed to GEMS Education;

- Facilitate remote or physical access to the computing device or the network, to individuals other than designated ICT administrators;
- Reconfigure or tamper the computing device in any way that could result in failure, degraded performance or limited operations of software and implemented security controls i.e., Anti-Malware, Mobile Device Management, and other software / security agents;
- Interrupt installation of security patches and operating system upgrades on computing devices through forceful shutdown;
- Use of portable storage on GEMS issued computing devices shall be prohibited. Portable storage includes but not limited to:
  - Portable USB
  - Flash drive
  - Memory cards
  - Re-writable CD

4.3.2 GEMS personnel other than designated ICT staff, shall not hold privileged access / administrator rights to computing devices, applications or to any other services hosted on GEMS networks;

4.3.3 GEMS personnel shall not utilize allocated computing devices for testing new software / applications. Software testing shall be performed on designated test workstations installed on isolated networks. Contact ICT helpdesk for test workstations;

4.3.4 GEMS personnel shall not utilize personally developed or student developed applications for processing business data (including Personally Identifiable Information).

4.4 Staff Passwords and User Accounts

4.4.1 GEMS provisions business tools and online subscriptions to its employees, which is controlled through a combination of user credentials (username and password). GEMS personnel shall exercise due care to prevent misuse of their allocated accounts.
GEMS personnel:

- Shall not share their credentials (username password combination) with anyone. This includes colleagues, contractors, senior staff, managers or ICT staff;
- Shall not reveal or list passwords over emails, chats, questionnaires, sticky notes, security forms or other any other medium;
- Shall change their password every 90 days and on their first logon;

- Shall not reuse passwords across personal and corporate accounts i.e., Utilize the same password across Facebook, google, GEMS corporate accounts and other portals;
- Shall not repeat last four passwords;
- Shall choose passwords that are complex and difficult to guess. Passwords shall comply with the following attributes:
  - Shall not be guessable (include names, name of your pet, similar to the username, birthdates, or other guessable parameters);
  - Shall not be composed of word or number patterns on the keyboard;
  - Password shall not be listed in hints on "Recover Password" questions;
  - Shall be at least eight characters in length and mandatorily include the following:
    - Include one upper case letter; ○ Include one number and; ○ Include one special character.

4.4.2 All personnel shall utilise Multi-Factor Authentication (MFA) to safeguard GEMS provided accounts.

- GEMS does not require the use of personal device for Multi-Factor Authentication. The user is provided options to select a preferred additional factor of authentication at the time of registration.
- For recovery or changes to the additional authentication factor, the user shall reach out to the ICT helpdesk.
- Similar to Passwords, GEMS personnel are prohibited from sharing the multifactor authentication token values with anyone.

4.4.3 GEMS personnel shall be responsible for all activity that occurs, from use of their accounts and allocated computing devices.

4.4.4 GEMS personnel shall report any suspicious activity or a suspected account compromise in accordance with the incident reporting section of this policy.

4.6 Secure Use of Internet (within GEMS premises)

4.6.1 Internet access by GEMS personnel shall be consistent with their business need. GEMS personnel shall not utilize Internet access provisioned within GEMS premises to perform activities that could endanger GEMS Education's reputation or classified as illegal as per national laws and regulations;

4.6.2 GEMS personnel shall not utilize the Internet access provided in GEMS premises to:

- Commit fraud, forgery, harassment, intimidation or impersonation;

-
- Post or share derogatory, libellous or threatening messages or images against an individual, race, religion, organization or community;
  Download, upload or access inappropriate, extremist or terrorism related materials, pornographic content, malicious software (malware) and pirated copies of software or entertainment media;
- Use peer-to-peer or torrent based applications;
- Use anonymity networks (TOR, VPN) or access dark web;
- Perform activities that could cause corruption, disruption or result in unauthorized access of data on third-party websites or services on the Internet i.e., activities classified as hacking or cracking;
- Cause "Denial of Service" i.e., Use Internet services in a way that disrupts or blocks the service for others;
- Commit copyright infringement;
- Provide third-parties, unauthorized access to GEMS network through use of Virtual Private Networks or remote access applications.

4.6.3 Internet access within GEMS premises shall be limited to web portals only. Access to Internet hosted services over non-standard protocols such as FTP, POP3, IMAP, RDP shall not be permitted;

4.6.4 Connecting to free public Wi-Fi hotspots for Internet access (cafés, hotel lobbies, airports) utilizing GEMS issued devices is not recommended;

4.6.5 Personal use of Internet within GEMS premises during business hours should be minimal and must not affect the individual's ability to perform their assigned responsibilities.

4.7 Secure Use of Electronic Communication

4.7.1 GEMS personnel should use their business email account with due care to avoid misuse. GEMS personnel shall not:

- 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;
- Share executable programs or scripts to internal or external recipients over email;
- Generate or forward chain mails containing derogatory, libellous or threatening messages, images against an individual, race, religion, organization or community;
- 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;

4.7.2 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 calls. All such requests should be promptly notified to ICT helpdesk and should not be complied with.

4.7.3 GEMS personnel shall not utilize personal email accounts for official communications.
GEMS Personnel:

- Shall not respond to any email, requesting GEMS official / corporate information received on their personal email accounts. This includes information related to other staff, parents or students;
- Shall not act on any email, with work related instructions received on their personal email accounts;

4.7.4 GEMS personnel are not permitted to utilize corporate email for personal correspondence;
NOTE: 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.

4.8 Secure Processing, Sharing and Storage of Data

4.8.1 GEMS personnel shall exercise due care in handling GEMS business data in their custody;

4.8.2 GEMS personnel are not authorized to copy or move GEMS business data:

- To personal storage, personal cloud storage or personal computing devices;
- To third-party online portals or cloud applications. Unless the third-party / service provider / vendor is contractually engaged with GEMS and contractually obligated to safeguard GEMS business data in the cloud (service providers / vendors environment);

4.8.3 GEMS Personnel responsible for selection of applications or third-party services that involve handling Personally Identifiable Information (PII), shall ensure:

- Due diligence is performed on the security posture of the application or the service provider prior to sharing / processing any data, providing access or integrating with any of the GEMS systems;
- A Data Processing Agreement (DPA) is included as part of the contract;

- The recipient organisation or the individual is made aware of the sensitivity of the data transferred, its confidentiality requirements and their obligation to use the data only for the designated purpose;
- All GEMS data is securely removed on completion or termination of the service contract;

4.8.4 GEMS personnel shall not share GEMS business data through unauthorized channels, i.e., personal email, messenger services, free to use data sharing and cloud storage platforms; e.g. Gmail, Yahoo mail, WhatsApp, Dropbox, WeTransfer, personal cloud storage accounts among others;
NOTE: GEMS reserves the right to restrict access to cloud storage platforms within its premises and systems.

4.8.5 GEMS personnel are not permitted to configure data shares on their local computing devices;

4.8.6 GEMS personnel shall only utilize GEMS issued Corporate Microsoft OneDrive cloud account or the GEMS school provisioned platform, to share data with relevant external business parties;

4.8.7 GEMS personnel are permitted to utilize approved storage location / platforms for storing business data. List of approved storage locations / platforms include:
- GEMS issued "OneDrive" accounts accessible using GEMS credentials or Cloud storage services provisioned by respective schools where Microsoft OneDrive is not utilized;
- Local storage on GEMS issued computing devices;

4.8.8 GEMS personnel shall exercise due care in handling printed copies of GEMS business data during the course of operations;

- GEMS personnel shall ensure printed document copies containing business data:
  - Are securely destroyed (shredded) after use;
  - Are securely stored / locked when not in use i.e., not left unattended overnight in open office or cubicles;
  - Are collected from printers in a timely manner. Unclaimed prints from printers, shall be securely disposed after closure of business every day;

4.8.9 GEMS personnel at schools shall utilize volume printing provisions for printing large document sets (Printing documents over 50 sheets or as classified by your respective school);

4.8.10 Monochrome dual sided printing has been configured as the default printing option. GEMS personnel are encouraged to utilize this configuration for all DRAFT printing purposes.

4.9 Backups

4.9.1 In order to ensure continuity of operations, GEMS personnel are responsible to store all business data in protected folders on their computing devices;

- GEMS personnel shall store their work files in protected folders 'Documents', 'Desktop' and 'Pictures'. Data stored in protected folders is automatically synchronized with GEMS issued corporate Microsoft OneDrive account;

- Under any circumstances GEMS personnel shall not backup files / data containing GEMS business data to personal storage (including Portable storage drives i.e. USB Hard Drives, Flash Drives or personal cloud storage accounts).
  NOTE: Refer OneDrive tutorials online on guidance to use OneDrive or contact your local ICT helpdesk for additional support.

4.10 BYOD (Bring Your Own Devices) for official use

4.10.1 GEMS personnel are permitted to register one personal handheld device (Mobile Phone) for GEMS official use under BYOD program. Vice President, Vice Principal and above are permitted two personal handheld devices;

4.10.2 Personal devices shall mandatorily comply with the following standards in order to be eligible for registration under BYOD program;

- Devices should be running a supported platform:
  - Android
  - IOS
- Devices should be covered by the manufacturer for security updates and host a supported version of the Operating System or an updated firmware;
- Devices should not be configured with privileged access i.e., jailbroken or rooted devices are not permitted to be registered;
- Device hardware or software should not be tampered with, infected with malware or have applications from unauthorized app-stores installed; *NOTE:*
  - *GEMS ICT reserves the right to withdraw a BYOD registered device or discontinue support to a specific platform if it is considered a security threat.*
  - *Supported platforms and versions are subject to change depending on evolving technology landscape. Contact ICT helpdesk for supported versions.*

4.10.3 Personal devices registered under BYOD shall be mandatorily enrolled in MDM (Mobile Device Management) solution approved and deployed by GEMS

ICT and utilize approved applications to ensure secure access and storage of GEMS business data;

4.10.4 GEMS personnel shall not modify, tamper, disable or uninstall the Mobile Device Management software and the security policies deployed on the BYOD registered personal devices;

4.10.5 GEMS personnel are responsible for the security updates, care maintenance and backup of the personal device registered under BYOD;

4.10.6 GEMS personnel shall promptly inform ICT Helpdesk for a temporary withdrawal from BYOD program, before handing the devices to external agencies for repairs / maintenance or disposal;

4.10.7 Lost or stolen devices shall be reported within 8 hours to the ICT helpdesk by the device owners;

NOTE: GEMS ICT reserves the right to secure erase lost or stolen device registered under BYOD program. GEMS Education will not be responsible for compensation or recovery of lost personal data on the device.

4.10.8 GEMS Education owns the right to all GEMS business data stored on personal devices;

NOTE: Contact your local ICT administrator to register your Personal device under BYOD program.

4.11 Remote Support and Access to Third Parties

4.11.1 GEMS personnel are not authorized to subscribe to third-party support for troubleshooting or management of applications and computing devices in GEMS network:

- Support and maintenance that requires third-party access to GEMS network or computing devices shall be logged and managed through ICT helpdesk;
- GEMS authorized ICT personnel shall monitor access by third-parties to the GEMS network or devices connected to GEMS networks;

Provisioning access without supervision to third-parties for computing devices that are connected to GEMS network is prohibited;

4.11.2 GEMS personnel shall not utilize unregistered or unlicensed software for remote access.

4.12 Social Media

4.12.1 GEMS personnel shall adhere to the following standards when using Social media in the context of GEMS (Corporate & Schools). GEMS Personnel:

- Shall refrain from representing personal views as those of GEMS on social media accounts;
- Shall not publish any information that is considered internal to GEMS on their personal social media accounts i.e., information containing commercial data, personal or health records of students or staff or any form of internal GEMS business or operational data;
- Are prohibited from responding to inquiries from general public and media personnel from their personal social media accounts. Any such inquiries shall be forwarded to authorized GEMS spokespersons or appropriate GEMS communication channels;
- Shall not create duplicate or shadow accounts representing GEMS, GEMS schools or any of its support services;

4.12.2 GEMS personnel authorized to handle official social media accounts that are sanctioned by, GEMS corporate, GEMS schools or any of the support services shall ensure:

- All accounts utilized for official GEMS communications are created by and registered with "Manager, Social Media" in the GEMS School Support Centre (Corporate Office);
- Official communication is performed utilizing GEMS sanctioned social media accounts and not through personal accounts;
- External website links / URL included within official posts are verified to be safe before posting i.e., the link does not contain inappropriate content and is not malicious in nature;
- They do not engage in non-professional private messaging or inappropriate communication with followers on official accounts;
- Obtain relevant approvals prior to posting pictures or any information related to employees, vendors, parents or students and must always be aware and avoid capturing or publishing pictures of the "no-photo" students at their school;
- They shall not post content considered inappropriate, offensive or harmful in nature. Example of such content includes but not limited to defamatory,

pornographic, libellous or offensive against an individual, race, religion, organization or community;

- Passwords for social media accounts adhere to corporate password guidelines; and Multi-Factor Authentication is activated on official Social Media accounts to prevent account hijacking;
  All requests for creating new social media page(s) for official GEMS representation shall be presented to, approved and created by "Manager, Social Media" in the GEMS School Support Centre (Corporate Office). *NOTE: Refer Marketing Process and Procedures for guidelines / processes on Social Media usage.*

  ○ *POLIT004 Social Media Usage 2016* ○ *GEMS Social Media Processes*.

4.12 Incident Reporting

4.12.1 GEMS personnel shall report all incidents to enable implementation of appropriate corrective actions. GEMS personnel should promptly report any of the following incidents to ICT helpdesk;

- Loss of GEMS business data through:
  ○ Lost / stolen GEMS provided computing device; ○ Loss of personal device registered under BYOD; ○ Lost storage device containing GEMS business data;
- Compromised credentials for GEMS corporate accounts under the individuals care;
- Suspicious system behaviour;
- Suspicious emails sent from GEMS account under the individuals care;
- Suspected malware;
- System misconfiguration or opportunities to circumvent implemented system controls discovered during the course of daily business operations;
- Suspicious devices attached to systems or network points;
- Suspicious / look-alike wireless networks visible in GEMS premises;
- Any identified violation of this policy;

4.13 Right to Change

4.13.1 GEMS, reserves the right to modify or amend this policy in accordance to applicable laws, regulations and corporate policies.

4.14 Right to Monitor and Enforcement

4.14.1 GEMS, reserves the right to monitor and

- Review the use of GEMS network and GEMS provided computing devices;
- Remove / uninstall applications, tools or data / content on GEMS provided computing devices that is in violation of GEMS policies and national laws;
- Block network access to devices and user accounts:
  - That are compromised;
  - That do not comply with GEMS policies or considered a security threat to GEMS network;

  Implement appropriate technology and tools on GEMS owned computing devices and networks to ensure compliance to GEMS policies;
- The tool agents include but not limited to: Mobile Device Management, Firewall, Anti-Virus, Future Digital agents and others.

5. Definitions

Business Data[1]: Includes business confidential information, Personal information of students, staff and parents, images clicked by staff within GEMS premises or any other data utilized in the course of daily operations that is internal to GEMS Education.

6. Roles & Responsibilities

6.1 The Company may update this policy at any time. It is the responsibility of every employee to be aware of and follow the policy currently in place.

6.2 It is the responsibility of the IT Department to develop, monitor, maintain and implement this policy.

7. Staff Awareness and Training

7.1 GEMS will make this policy available on the GEMS intranet for all employees. It is the responsibility of the employees to abide by the policy guidelines.

8. Breach of this policy

8.1 All staff of the Company, including permanent staff, management, volunteers, consultants, officers and temporary staff, are responsible for complying with this Policy.

8.2 Any breach of this Policy could potentially result in disciplinary action, which may include termination of employment. Please refer to the Employee Discipline Policy for more information.

9. Appendices

- N/A