Multinational School

ICT Acceptable Use Policy

Document Control	
Date created	November 2021
Department responsible	IT
Revised Date	Dec 2021
Date of approval by Board of Directors	
Date of implementation	September 2021
Review cycle	Yearly
Date of next review	Dec 2022

Table of Contents

1. Introduction

1.1 Purpose

The Multinational School – Bahrain seeks to promote and facilitate the proper and extensive use of Information and Communication Technology (ICT) for the sole purpose of supporting the teaching, learning and research activities of the school. Technology is a vital resource to the educational process and to protect this valuable resource, this policy has been created to foster and protect the educational and instructional needs of the school.

It is the responsibility of all Users of the school's IT services to read and understand this policy.

The policy relates to all IT facilities and services provided by the Multinational School – Bahrain.

This document will be reviewed at least annually by the school Management and updated as required in order to comply with legal and policy requirements.

1.2 Scope

This policy applies to all Users utilising the Multinational School - Bahrain's IT facilities and services:

- Multinational School – Bahrain Staff.
- Multinational School – Bahrain Students.
- Parents / Guardians of MNS Students.
- Visitors, contractors and others.

1.3 Exercise of Control

The Multinational School Bahrain may exercise, cause, create, or put into effect any controls which it determines – in its sole and absolute discretion – are necessary to enforce this policy or to otherwise ensure system stability, reliability or integrity.

1.4 Copyrights and License Agreements

Software and data may be provided to you by the School which has been obtained by various contracts and/or licenses. Take care to use software legally in accordance with both the letter and spirit of relevant licensing and copyright agreements. Copying software for use outside these agreements is illegal and may result in criminal charges.

1.5 Code of Conduct

The conduct of all Users when using the school's IT facilities and services should always be in line with the school's values, including the use of online and social networking platforms.

All Users of the school's IT facilities and services are expected to act responsibly, be courteous, to show consideration and respect to others.

Examples of unacceptable and/or inappropriate use includes but not limited to:

- Gaining unauthorized access to resources, data or entities.
- Degrading or disrupting equipment or systems performance.
- Creating, modifying, or wilfully disseminating computer viruses, spyware, adware, or other damaging programs.
- Violating system and infrastructure security.
- Using the account of another user.
- Vandalizing the data of another user.
- Invading the privacy of others.
- Posting threatening or bullying comments or pictures.
- Students using their own hotspot.
- Sending spam or mass emails or postings.
- Falsifying an email message.
- Sharing any school materials with any person outside MNS Bahrain without consent.
- Wilfully damage or tamper with any IT equipment.
- Searching for In app Information.
- Use of VPN service for activities of private gain.

1.6 Security

- Do not attempt to gain unauthorised access to information or facilities.
- Do not disclose personal system passwords or other security details to other staff, volunteers or external agents and do not use anyone else's login; this compromises the security of the Multinational School - Bahrain. If someone else gets to know your password, ensure you change it or get IT Support to help you **(Note2)**.
- Information about people: If you're recording or obtaining information about individuals make sure you are in compliance with the school Data Protection Policy and local legislation. Please contact the IT Assistant Manager for more help with this.
- You are a representative of the Multinational School - Bahrain when you are on the Internet or using email:
  - Make sure your actions are in the interest (and spirit) of the Multinational School - Bahrain and do not leave the Multinational School - Bahrain open to legal action (e.g. liable).
  - Avoid trading insults with other people using the Internet with whom you disagree.
  - Obscenities/Pornography: Do not write it, publish it, look for it, bookmark it, access it or download it.
- 'Electronic monitoring': Any information available within IT facilities must not be used to

monitor the activity of individual staff in anyway (e.g. to monitor their working activity, working time, files accessed, Internet sites accessed, reading of their email or private files etc.) without their prior knowledge. Exceptions are:

- In the case of a specific allegation of misconduct, when the Principal/ Head of School can authorise accessing of such information when investigating the allegation.
- when the IT Support section cannot avoid accessing such information whilst fixing a problem.

In such instances, the person concerned will be informed immediately and information will not be disclosed wider than is absolutely necessary. In the former case their access to IT facilities may be disabled pending investigation.

1.7 Violations

Deliberate and serious breach of the policy will lead to disciplinary measures which may include restriction or revocation of access to technology resources, either for a period of time or permanently, or even extreme disciplinary measures, as appropriate, being taken.

In order to make sure that all Users understand and agree to this policy, all Users stated in the scope of this policy, are asked to sign the ICT Acceptable Use Policy (AUP) Form.

If the form agreeing to the terms of this policy is not returned to the school, agreed by the student and a parent by the deadline that has been set, then the student will not be permitted to access any computers or other networked electronic devices at the school.

2. MNS Email

All MNS Staff and Students will be provided with MNS email accounts.
Students will be taught how to use email as communication tool.

2.1 When to use email

Use it in preference to paper to reach people and to help reduce paper use. Think and check messages before sending.

2.2 Use of Distribution Lists

- Only send Email to those it is meant for; do not broadcast (i.e. send to large groups of people using email aliases) unless absolutely necessary since this runs the risk of being disruptive. Continuous sending of junk or spam email will result in a higher risk of your regular emails being ignored by your peers.
- Use the standard aliases **(Note 4)** for work related communication only.
- If you wish to broadcast other non-work related information or requests (e.g. information or opinions on political matters outside the scope of the Multinational School - Bahrain's campaigning, social matters, personal requests for information etc.) it is better to use a

Webmail account **(Note 4)** or a personal email account at home; you should not use the standard (work) aliases.

- Keep the Multinational School - Bahrain's internal email aliases internal. If you are sending an email both to the Multinational School - Bahrain alias and outside of the Multinational School - Bahrain, use the alias as a blind carbon copy (i.e. the bcc address option) so that the external recipient does not see the internal alias.
- Do not broadcast emails with attachments to large groups of people - either note in the email where it is located for recipients to look, or include the text in the body of the email. Failure to do this puts an unnecessary load on the network.

2.3 General Points on Email Use:

- When publishing or transmitting information externally be aware that you are representing the Multinational School - Bahrain and could be seen as speaking on the Multinational School - Bahrain's behalf. Make it clear when opinions are personal. If in doubt, consult your supervisor.
- Check your in-tray at regular intervals during the working day.
- Keep your in-tray fairly empty so that it just contains items requiring your action. Try to decide what to do with each email as you read it (e.g. delete it, reply to it, save the whole email in a folder, or extract just the useful information and save it somewhere logical).
- Keep electronic files of electronic correspondence, only keeping what you need to. Don't print it off and keep paper files unless absolutely necessary.
- Use prefixes in the subject box whenever appropriate (Note5).
- Treat others with respect and in a way you would expect to be treated yourself (e.g. don't send unconstructive feedback, argue or invite colleagues to publicize their displeasure at the actions / decisions of a colleague).
- Do not forward emails warning about viruses (they are invariably hoaxes and IT Support will probably already be aware of genuine viruses - if in doubt, contact them for advice.

2.4 Email Etiquette:

- Being courteous is more likely to get you the response you want.
- Do address someone by name at the beginning of the message, especially if you are also copying another group of people.
- Make your subject headers clear and relevant to your reader(s)
- e.g. don’t use subject headers like "stuff"; don't send a subject header of, say "accounts" to the accountant
- Try to keep to one subject per email, especially if the content is complex.
- It is better for your reader(s) to have several emails on individual issues, which also makes them easy to file and retrieve later.
- One email covering a large variety of issues is likely to be misunderstood or ignored.
- Using asterisks at each end of a word (e.g. *now*) is common practice for highlighting text.
- Capitals (e.g. NOW) can also be used to emphasize words, but should be used sparingly as it commonly perceived as 'shouting'.

- Don't open email unless you have a reasonably good expectation of what it contains.
- Alert IT Support if you are sent anything like this unsolicited. This is one of the most effective means of protecting the Multinational School - Bahrain against email virus attacks.
- Keep email signatures short.
- Your name, title, phone/fax and web site address may constitute a typical signature.
- Understand how forwarding an email works.
- If you forward mail, it appears (to the reader) to come from the originator (like passing on a sealed envelope).
- If you forward mail *and edit it* in the process, it appears to come from you - with the originator's details usually embedded in the message. This is to show that the original mail is no longer intact (like passing on an opened envelope).

3. Installing Software

Get permission from IT Support before you install any software (including public domain software (**Note6**) on equipment owned and/or operated by the Multinational School – Bahrain.

4. Data Transfer and Storage on the Network

Keep master copies of important data on the Multinational School - Bahrain's network and not solely on your PC's local C: drive or floppy discs. Otherwise, it will not be backed up and is therefore at risk. Ask for advice from IT Support if you need to store, transmit or handle large quantities of data, particularly images or audio and video. These large files use up disc space very quickly and can bring your network toa standstill. Be considerate about storing personal (non-Multinational School - Bahrain) files on the Multinational School - Bahrain's network. **(Note7).**

Don't copy files which are accessible centrally into your personal directory unless you have good reason (i.e. you intend to amend them or you need to reference them and the central copies are to be changed or deleted) since this uses up disc space unnecessarily.

NB Staff may not save MNS documents to the desktop or hard drive of their device. All such documentation or work must be secured on the MNS server or on the OneDrive should access be required after hours. Failure to do so will result in disciplinary action.

All staff are required to back up their information onto their own OneDrive cloud storage. The IT Department will guide you on how to set up your OneDrive and enable Auto-Save that will Backup: **Desktop, Documents & Pictures.** Backup is under the staff responsibility and failure to do so could result in disciplinary action.

5. Laptops / iPads / Tablets / School Devices

These devices are workplace devices and are to be used in an appropriate manner. Students should never leave their loaned devices unattended. If a loaned device is damaged or lost, the parent/student will be responsible for the cost of repair or replacement of the device.

Care of Equipment:

- Do not re-arrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.) without first contacting IT Support.
- Do not take food or drink into rooms which contain specialist equipment like servers. Access to such rooms is limited to authorized staff.

6. Use of Facilities for Leisure or Personal Purposes

For example, sending and receiving personal email, playing computer games and browsing the Internet is permitted so long as such use does not:

- Incur specific expenditure for the Multinational School – Bahrain.
- Impact on your performance of your job (this is a matter between each member of staff and their supervisor.
- Break the law.
- Bring the Multinational School - Bahrain into disrepute.
- Open your device to malicious attack or render its performance sub-par.

7. IT Request Logging Procedure

The Multinational School - Bahrain makes use of an electronic ticket based incident management system. In order for a ticket **Email: ITHELPDESK@MNS-BAHRAIN.COM** with your request. Once your incident is logged a ticket will be generated and you will be emailed the necessary details. This ticket number can then be used to track the status of your request.

Notes

(1) In-house software: This is software written by staff or volunteers using the Multinational School - Bahrain's equipment. It is the Multinational School - Bahrain's property and must not be used for any external purpose. Software developers (and students) employed at the Multinational School - Bahrain are permitted to take a small "portfolio" of such in-house software source code/executables, which they may have developed, for use in subsequent work, subject to agreement with the IT Assistant Manager.

(2) Personal passwords: Disclosure to other staff, volunteers or external agents:

(3) This may be necessary in some circumstances. Such a practice is allowed only if sanctioned by a member of the Management Team after discussion with the IT Support. If the password is disclosed for a one-off task, the owner must ensure that his / her password is changed (by contacting IT Support) as soon as the task is completed.

(4) Email aliases are pre-defined 'shortcuts' for distributing internal email to specific groups of people. IT Support can tell you what these are and how to use them.

(5) Webmail accounts are personal email accounts that are stored on the Internet and can be accessed from anywhere with a standard browser, e.g. home or cybercafe. IT Support can advise you on setting up such an account.

(6) Subject box prefixes: These are ''U:' for Urgent', 'FYI' for your information and 'AC:' requires

action. If the email is a very brief message confined solely to the subject line, it should in addition be prefixed with '**' to indicate "just read this line".

(7) Public domain software or Freeware: This is software that is available free of charge, usually by downloading from the Internet.

(8) Laptop Data: Your school device is not your personal device to store personal information and pictures. You are requested to delete them as IT Department is not responsible for the data loss or deletion of your personal data.

8. Remote Access

8.1 Overview

Remote access to our corporate network is essential to maintain our Team's productivity, but in many cases this remote access originates from networks that may already be compromised or are at a significantly lower security posture than our corporate network. While these remote networks are beyond the control of Multinational School Bahrain policy, we must mitigate these external risks the best of our ability.

8.2 Purpose

The purpose of this policy is to define rules and requirements for connecting to Multinational School Bahrain's network from any host. These rules and requirements are designed to minimize the potential exposure to Multinational School Bahrain from damages which may result from unauthorized use of Multinational School Bahrain resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Multinational School Bahrain internal systems, and fines or other financial liabilities incurred as a result of those losses.

8.3 Scope

This policy applies to remote access connections used to do work on behalf of Multinational School Bahrain, including reading or sending email and viewing intranet web resources. This policy covers any and all technical implementations of remote access used to connect to Multinational School Bahrain networks.

8.4 Policy

It is the responsibility of Multinational School Bahrain employees, contractors, vendors and agents with remote access privileges to Multinational School Bahrain's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Multinational School Bahrain.

General access to the Internet for recreational use through the Multinational School Bahrain network is strictly limited to Multinational School Bahrain employees, contractors, vendors and agents (hereafter referred to as "Authorized Users"). When accessing the Multinational School

Bahrain network from a personal computer, Authorized Users are responsible for preventing access to any Multinational School Bahrain computer resources or data by non-Authorized Users. Performance of illegal activities through the Multinational School Bahrain network by any user (Authorized or otherwise) is prohibited.

The Authorized User bears responsibility for and consequences of misuse of the Authorized User's access. For further information and definitions, see the Acceptable Use Policy.

Authorized Users will not use Multinational School Bahrain networks to access the Internet for outside business interests.

For additional information regarding Multinational School Bahrain's remote access connection options, including how to obtain a remote access login, free anti-virus software, troubleshooting, etc., go to the Remote Access Services website (company url).

8.5 Requirements

- Secure remote access must be strictly controlled with encryption (i.e., Virtual Private Networks (VPNs)) and strong pass-phrases. For further information, see the Acceptable Encryption Policy and the Password Policy.
- Authorized Users shall protect their login and password, even from family members.
- While using a Multinational School Bahrain-owned computer to remotely connect to Multinational School Bahrain 's corporate network, Authorized Users shall ensure the remote host is not connected to any other network at the same time, with the exception of personal networks that are under their complete control or under the complete control of an Authorized User or Third Party.
- Use of external resources to conduct Multinational School Bahrain business must be approved in advance by InfoSec and the appropriate business unit manager.
- All hosts that are connected to Multinational School Bahrain internal networks via remote access technologies must use the most up-to-date anti-virus software (place url to corporate software site here), this includes personal computers. Third party connections must comply with requirements as stated in the Third Party Agreement.
- Personal equipment used to connect to Multinational School Bahrain's networks must meet the requirements of Multinational School Bahrain-owned equipment for remote access as stated in the Hardware and Software Configuration Standards for Remote Access to Multinational School Bahrain Networks.

8.6 Compliance Management

The Team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, internal and external audits, and inspection, and will provide feedback to the policy owner and appropriate business unit manager.

9. GUIDELINES

9.1 Cyberbullying – a serious matter

- Employers / their representatives have a duty of care to protect everyone in the community from cyberbullying, and failure to “take reasonable care” will be considered negligence.

- In situations where the school/workplace authority or individual employees know or realize that children/employees/others may be harmed, the duty of care can be extended beyond normal school or working hours.

- Employers / their representatives should effectively communicate to their stakeholders that engaging in cyberbullying can have serious consequences including an individual being the subject of a police criminal investigation.

9.2 School / workplace cyberbullying policies:

Each year, individual students/employees/relevant others should sign an "Acceptable Use Policy" regarding the proper use of all available technologies in the school/workplace.

9.3 Recommended strategies for individuals to respond to instances of cyberbullying:

The following general strategies are recommended for helping victims of cyberbullying:

• Report all cyberbullying or hostile behaviour in cyberspace, including intentional exclusion, to the appropriate parent, trusted adult, line manager, or school / workplace authority.

• Do not reply to further messages / posts from the bully and, if possible, block their mobile number or email address.

9.4 Summary of direct action options when responding to cyberbullying in school or T1 MNS workplaces

Where the cyberbullying contains	*then the action to be taken may include*	*and responsibility for such action lies with the*
Bullying	(If committed by a student) • Communication with parents • Suspending / performing other actions (as per school and / or system policy) • Counselling	• PRINCIPAL / DELEGATE OF THE PRINCIPLE who can decide to notify the school principal / school leadership team. (depending on the severity of the incident (s))
	(If implemented by employees) • Initiate care policy • Initiate the process of anti-discrimination, harassment and bullying policies. • Counselling	• PRINCIPAL (for school employees) Who informs the school leadership team /management committee executive (advising the principal as appropriate), who in turn can choose to inform the Board of T1 MNS (depending on the severity of the incident). • Safeguarding Officer
	(Unless committed by a student / employee) • Report to the safeguarding committee	• PRINCIPAL (for offenses at school) which notifies the School Leadership Team / Board Members (if necessary, advice given to the principal) who in turn may decide to notify the Board (depending on the severity of the incident / incidents) • Safeguarding Officer
Overt sexual content	(If committed by a student) • Contact child protection authorities • Contact parents • Suspend/take other actions (according to school and/or system policy) • Counselling	• PRINCIPAL which notifies the School Leadership Team / Board Members (if necessary, advice given to the principal) who in turn may decide to notify the Board (depending on the severity of the incident / incidents)
	(If committed by an employee) • Safeguarding Committee and Behavioural committee • Counselling	• PRINCIPAL which notifies the School Leadership Team / Board Members (if necessary, advice given to the principal) who in turn may decide to notify the Board (depending on the severity of the incident / incidents)

	(If committed by other than a student / employee) • Contact the lead of the safeguarding committee	• PRINCIPAL (for offenses at school) which notifies the School Leadership Team / Board Members (if necessary, advice given to the principal) who in turn may decide to notify the Board (depending on the severity of the incident / incidents)
Threats to life / sexual assault / child protection offences / other criminal activity	(If Committed by a student) • Contact the police (mandatory) • Contact child Protection authorities • Contact parents • Suspending / performing other actions (as per school and / or system policy) • Counselling	• PRINCIPAL which notifies the School Leadership Team / Board Members (if necessary, advice given to the principal) who in turn may decide to notify the Board (depending on the severity of the incident / incidents)… who then steps back and allows Police investigation to run its course … who then considers school / system response according to policy should the Police investigation find no case to answer
	(If Committed by an employee) • Contact the police (mandatory) • Initiate care police • Counselling	• PRINCIPAL (for school employees) …which notifies the School Leadership Team / Board Members (if necessary, advice given to the principal) who in turn may decide to notify the Board (depending on the severity of the incident / incidents)… who then steps back and allows Police investigation to run its course … who then considers school / system response according to policy should the Police investigation find no case to answer
	(If Committed by other than a student / employee) • Contact the police (mandatory)	PRINCIPAL (for offenses at school) which notifies the School Leadership Team / Board Members (if necessary, advice given to the principal) who in turn may decide to notify the Board (depending on the severity of the incident / incidents)… who then steps back and allows Police investigation to run its course