1. Introduction:

Modern Knowledge Schools is committed to providing a safe and secure technological environment for students, staff, and stakeholders. These General Guidelines for Acceptable Use of Technology are designed to ensure responsible, ethical, and lawful use of the school's technology resources.

2. Purpose:

These guidelines outline the expectations, responsibilities, and standards for using technology resources within Modern Knowledge Schools. The purpose is to:

- Safeguard the integrity and security of the school's digital assets.
- Promote responsible and respectful technology use.
- Foster a conducive learning and working environment.
- Ensure compliance with legal and ethical standards.

3. User Responsibilities:

3.1. General Responsibilities:

- Users must adhere to all applicable laws and regulations, including but not limited to laws regarding hacking, harassment, and copyright.
- Users should demonstrate ethical behavior and respect for others, both online and offline.

3.2. Security and Passwords:

- Users must protect their passwords and accounts from unauthorized access. This includes:
    - Creating strong passwords with a combination of letters, numbers, and special characters.
    - Changing passwords regularly.
    - Not sharing passwords with anyone.
- Unauthorized attempts to access accounts, even those of others, are strictly prohibited.

3.3. Personal Data Protection:

- Users should respect the privacy of others and not share personal information without consent. This includes:
    - Not sharing personal contact information or sensitive data without explicit permission.
    - Being cautious about sharing photos or videos of others.
- Safeguard sensitive information, such as CPR numbers or financial details, and avoid sharing it online.

3.4. Respectful and Responsible Use:

- Users should engage in responsible and respectful communication. This includes:
    - Avoiding cyberbullying, harassment, or discriminatory language or actions.
    - Treating others with kindness and empathy online.
    - Reporting any instances of cyberbullying or harassment.
    - Not engaging in online activities that could harm the reputation of the school or its members.
    - Always use appropriate language.
    - Do not transmit language/ material that are profane, obscene, abusive, threatening, or offensive to others.
    - Do not send mass emails, chain letters or spam.
    - Students should maintain high integrity with regard to email and digital content.
    - No private chatting during class without permission, then only on Hangouts.
    - Accessing social media, streaming sites, proxy sites, gaming platforms, and adult content for purposes which are not directly related to instruction is strictly prohibited.
    - K12 data is subject to inspection by the school Technology Director

4. Prohibited Activities:

- Unauthorized access to data or networks includes:
    - Attempting to access someone else's accounts, files, or emails.
    - Hacking or using hacking tools.
    - Attempting to bypass security measures.
- Malicious software installation or distribution includes:
    - Not installing any software or apps on school-owned devices without

permission.
    - Not downloading or sharing files that may contain viruses or malware.
- Engaging in activities that disrupt network services or harm the school's reputation includes:
    - Not engaging in activities that consume excessive bandwidth (e.g., streaming videos during class hours).
    - Not engaging in any online activities that could damage the school's reputation, including posting inappropriate content or engaging in cyberbullying.
- Violation of copyright or intellectual property rights includes:
    - Respecting copyright laws and not copying or distributing copyrighted materials without permission or proper attribution.
    - Citing sources and providing proper attribution when using others' work in school projects.

5. Network and Device Usage:

5.1. Network Access:

- Access to the school's network is for the educational goals and objectives of Modern Knowledge Schools and the Ministry of Education in Bahrain. This includes:
    - Using the network for research, assignments, and educational activities.
    - Not using the network for personal, recreational, or commercial purposes.
    - Not using the network to access inappropriate or restricted content.
- Access to any non-instructional content which includes but not limited to gaming, streaming, downloading, social media and use of VPNs and site/content unblockers while in the school campus is strictly prohibited. Bandwidth-heavy activities should not disrupt network performance. This includes:
    - Avoiding activities that may slow down the network for others, such as large downloads or streaming during peak usage times.
    - Not using network resources for activities unrelated to education.
- Illegal downloads, streaming, or sharing of inappropriate content are strictly prohibited. This includes:
    - Not engaging in any illegal downloading, streaming, or sharing of copyrighted materials.
    - Not accessing or distributing inappropriate, explicit, or harmful content.

5.2. Device Usage:

Modern Knowledge Schools enforces strict device requirements as follows:

For Grades 1 to 5 (G1-G5):

All students in these grades are mandated to utilize exclusively licensed iPads that meet the minimum acceptable specifications.

For Grades 6 to 10 (G6-G10):

All students in these grades are obligated to employ solely licensed Chromebooks that meet the minimum acceptable specifications.

For Grades 11 to 12 (G11-G12):

All students in these grades are compelled to utilize solely licensed Chromebooks, Windows Laptops, or MacBooks.

This policy is implemented to ensure uniformity, security, and efficiency in our educational technology environment.

- School-managed devices should be used for educational purposes. This includes:
    - Using school-managed devices responsibly and for their intended purpose.
    - Not tampering with or attempting to modify school-managed devices.
    - Reporting any issues with school-managed devices to the IT department.
- Personal devices for non-students may be used in compliance with these guidelines. This includes:
    - Using personal devices responsibly and for educational purposes.
    - Ensuring personal devices are free from malware or viruses that could harm the school's network or other devices.
    - Not using personal devices for activities that violate these guidelines.

5.3. Device Management and Security

School-issued and school-managed devices, including iPads enrolled in Jamf Pro and Chromebooks enrolled in the school’s device management system, remain under the school’s administrative control for as long as they are enrolled.

All security settings, content restrictions, web filtering, application controls, and monitoring features apply continuously while the device remains enrolled, regardless of school days, weekends, holidays, or school breaks.

Device management profiles and configurations are an integral part of the school's digital learning environment and must not be removed, altered, or bypassed by users or parents. Any change to device enrollment status or removal of management can only be performed by the school's IT Department.

Purpose and Rationale

These controls are implemented to ensure the safety, security, and integrity of the school's digital ecosystem at all times. School-managed devices form part of a protected learning environment designed to safeguard students from inappropriate content, cyber threats, data loss, and unauthorized access.

Maintaining consistent management across all periods ensures safeguarding compliance, supports academic integrity, and prevents security gaps that may arise if protections are disabled outside school hours.

5.4. Software and Applications:

- Only authorized software and applications should be installed and used. This includes:
    - Seeking permission from IT or school authorities before installing any software or apps on school-managed devices.
    - Not downloading or using unapproved software or apps on school-managed devices.
    - Ensuring that any software or apps used on personal devices do not pose security risks or violate these guidelines.
- Piracy or unauthorized distribution of software is strictly prohibited. This includes:
    - Not engaging in software piracy, which includes downloading or sharing software without proper licenses or permission.
    - Reporting any instances of unauthorized software distribution.

All devices connected to the school network must follow the rules and restrictions enforced by the IT department, which gets updated regularly to ensure that the guidelines stated in this policy are followed.

6. Online Communication:

6.1. Email:

- School email should be used for school-related communication. This includes:
    - Not using school email accounts for personal or non-educational purposes.
    - Being professional and respectful in all school-related email communication.
    - Reporting any suspicious or phishing emails to school authorities.
- Users should be cautious about sharing sensitive information via email. This includes:
    - Not sharing sensitive personal information (e.g., home addresses, phone numbers) via email.
    - Not sending sensitive documents or files without proper encryption or security measures.

6.2. Social Media:

- Responsible and respectful use of social media is expected. This includes:
    - Treating others with kindness and respect on social media platforms.
    - Not engaging in cyberbullying, harassment, or defamatory behavior on social media.
    - Not sharing inappropriate or harmful content on social media.
    - Not using social media to harm the school's reputation or its members.

7. Intellectual Property and Copyright:

- Users must respect intellectual property rights and copyright laws. This includes:
    - Seeking permission or proper attribution when using others' work in school projects.
    - Not copying or distributing copyrighted materials without permission.
    - Reporting any instances of copyright infringement or plagiarism.

8. Reporting Violations:

- Users should promptly report any violations or suspicious activities to school authorities. This includes:
    - Reporting any instances of cyberbullying, harassment, or inappropriate behavior.

- Reporting security breaches or unauthorized access to accounts or devices.
- Cooperating fully with any investigations related to violations.

9. Consequences of Non-Compliance:

- Non-compliance with these guidelines may result in disciplinary actions, including but not limited to:
  - Temporary or permanent loss of technology privileges.
  - Suspension or expulsion, depending on the severity of the violation.
  - Legal action in cases of serious offenses, such as hacking or cyberbullying.

Violations may result in a suspension of technology resource access, with potential additional disciplinary measures in accordance with established guidelines for inappropriate language or behavior. The severity of action taken will vary:

- First Offense: A two-school-day suspension of technology resources, including Gmail account suspension.
- Second Offense: A one-week suspension of technology resources. Parental conference required for account reinstatement.

These consequences serve as a reference, with the final decision resting with the school principal, based on the disciplinary committee's recommendation. The administration, in coordination with the Technology Department, retains the right to assess each case's severity and determine appropriate disciplinary actions.

10. Privacy:

- Modern Knowledge Schools respects and upholds the privacy of its users.

11. Review and Updates:

- These guidelines will be periodically reviewed and updated to ensure relevance and compliance.

By adhering to these General Guidelines for Acceptable Use of Technology, we can create a safe and productive technological environment that benefits all members of our school community. Your compliance is essential to maintaining the integrity and security of our digital resources.

Upon signing this document, I hereby acknowledge:

1. Receipt of the device in acceptable condition.
2. I acknowledge that I am fully responsible for any damage or loss of the device assigned to me. The school will not cover any repair or replacement costs. In the event of loss, the IT department's role is limited to placing the device in lost mode, and recovery will be my sole responsibility.
3. My acceptance and commitment to adhere to the outlined guidelines.
4. My awareness of the MKS Technology Users Policy, accessible on the school website at https://mks.edu.bh/technology-department/.

_____	_____
Parent Name (Printed)	Student's Name (Printed)
_____	_____
Signature	Date