MINISTRY OF EDUCATION

ACCEPTABLE DEVICE AND TECHNOLOGY USE POLICY (STAFF)

SECTION 1 POLICY STATEMENT

Extensive ICT infrastructure has been supplied to the school system. All public schools have Internet connectivity and are equipped with computer laboratories at both the primary and secondary level. Further, primary level students are being afforded access to tablets and secondary level students access to Chromebook's and laptops. This is complemented by the commencement of initiatives to supply teachers with devices (e.g., tablet, laptop) which complement that used by their students. Consequently, the primary policy focus of the Ministry of Education is to ensure optimal use, care, maintenance, timely replacement, and environmentally responsible disposal of this ICT infrastructure. From this perspective, the following policy commitments are noted:

1. The Ministry considers use of technology resources to be a privilege that is granted on the condition that each member of the education sector respects the integrity of information technology resources and the rights of other users. The Ministry of Education St. Kitts and Nevis will take a system-wide approach to information security to help identify and prevent the compromise of information security and the misuse of MoESKN technology.

2. Ministry of Education is dedicated to providing equal opportunity for all students and employees, including those with disabilities. This includes providing equal access to information and communication technologies (ICT) such as devices, intranet, Internet, websites, electronic documents, and educational and training materials.

Right to Update this Acceptable Use Policy

Because technology, and our intended use of technology are continually evolving, the Ministry of Education reserves the right to change, update, and edit its technology policies at any time in order to meet procedural and instructional needs, while protecting the safety and well-being of our students and community. To this end, the Ministry of Education may add additional rules, restrictions, and guidelines at any time.

SECTION 2 PURPOSE AND CONTENT

The purpose of this policy is to provide Ministry of Education employees with guidance on the proper use of education sector information technology resources, including but not limited to the Internet, the Intranet, email, cell phones and the local digital network and supporting systems and the data transmitted on those systems.

Though the Ministry provides certain technologies, we recognise that members and guests of our community also have their own technology devices that they bring to our school campuses and school events. Our policies address the appropriate use of both technologies provided by the school and personally owned technological devices.

All users should be sure to read and understand the policies below before using the school's network and other technologies, as well as any personally owned technology. Use of school technology resources will imply understanding and agreement to the terms set forth in this policy.

SECTION 3 DEFINITIONS

Bandwidth

Bandwidth is a measure of the amount of data that can be transmitted in a fixed amount of time.

Copyright

The exclusive legal right to reproduce, publish, sell, or distribute the matter and form of something (such as a literary, musical, or artistic work.

Cyber-Bullying

Cyber-bullying is when someone sends derogatory or threatening messages and/or images through a technological medium in an effort to ridicule or demean another. Cyber-bullying also takes place when someone purposefully excludes someone else online. Cyber-bullying also takes place when someone creates a fake account or website impersonating, criticizing or making fun of another.

Hate Literature / Speech

Any kind of communication in speech, writing or behaviour, that attacks or uses pejorative or discriminatory language with reference to a person or a group on the basis of who they are, in other words, based on their religion, ethnicity, nationality, race, colour, descent, gender or other identity factor.

Mobile Device

For purposes of this policy, a Mobile Device is any portable electronic device which provides some of the functions of a computer such as a tablet, cell phone, music player, camera etc.

Network

The network is defined as the school's computers, mobile devices, and other digital electronic equipment (such as printers/copiers, interactive whiteboards, projectors, etc.), and the wired and/or wireless communications network on which they operate.

Plagiarism

Presenting work or ideas from another source as your own, with or without consent of the original author, by incorporating it into your work without full acknowledgement. All published and

unpublished material is covered under this definition, as is the use of material generated wholly or in part through use of artificial intelligence. Plagiarism can also include re-using your own work without citation.

Spam

Spamming is sending an unnecessary and unsolicited message to a large group of people.

User

For the purposes of this policy, user is an inclusive term meaning anyone who utilizes or attempts to utilize technology owned by the school. This includes students, faculty members, staff members, parents, and any visitors to the campus.

SECTION 4 DEVICE ISSUANCE and CARE

PART A: Device Issuance

The Ministry of Education St Kitts and Nevis (MoESKN) believes that the use of Information and Communication Technologies (ICTs) play a central and transformational role in ensuring that our students and teachers are allowed to learn, work and function in a technology-rich environment.

Technology devices are provided to staff by the Ministry of Education (MoE) to enhance work efficiency and facilitate the completion of basic educational activities. Devices are issued by the MoE for a period based on the following:

- device type,
- duration of the device warranty period (1 year for tablets and 2 years for laptops), and
- post of recipient

All teachers enrolled in a public school will be provided with a device that enhances their work productivity and supports their instruction in the classroom. Teacher devices are meant to complement student learning by enhancing student engagement, providing access to an array of educational resources, promoting personalized learning, and fostering collaboration, ultimately leading to improved student outcomes.

Once accepted, all staff issued or receiving a device must adhere to the guidelines set forth in this document. MoE technology administrators retain the right to inspect and collect the device at any time and to alter, add or delete installed software or hardware. This includes spot checks throughout the school year. The necessity to collect devices and related equipment, at any time during the year or at the end of the school year, is at the discretion of the (MoESKN) administration. Upon request, staff should be able to provide the device, as well as all related equipment issued with the device. Failure to do so will result in a replacement charge.

PART B: Device Care

1. The device is not to be altered in physical form at any time by the user. No stickers, decorations or markings or any kind may be applied to the device or related equipment.
2. The attempted opening of an MoE issued device by users is strictly prohibited. The unauthorized opening of devices will result in the voiding of the applicable device warranty.
3. Extreme care should be taken when transporting devices. Heavy items and device peripherals (e.g., power cords and adapters) should be secured separately when transporting the device to avoid potential damage.
4. Any attempt to gain administrative credentials on any MoE device or system will not be tolerated and is subject to discipline as determined by administration.

User Responsibilities

All users are responsible for:

1. Registering their electronic device with the school and submitting a signed Use of Electronic Devices Agreement prior to connecting to the school network.
2. Ensuring electronic devices are used in accordance with school policies and procedures.
3. Caring, maintaining, securing, and storing electronic devices.
4. Preserving privacy of accounts, login names, passwords, and/or lock codes to maintain security of electronic devices and data.
5. Maintaining safe and productive learning environments when using electronic devices.
6. Practising digital citizenship.

All administrators are responsible for:

1. Informing users of the MoE policy on Acceptable Device and Technology Use.
2. Establishing and monitoring digital citizenship.
3. Responding effectively to disciplinary issues resulting from inappropriate electronic device usage.
4. Communicating appropriately with school personnel, parents, and students if MoE policy is violated from electronic device usage.
5. Providing information to users explaining how to connect electronic devices to the school network.

Teachers are responsible for:

1. Creating equitable learning opportunities that include electronic devices for education purposes when relevant to curriculum and instruction.
2. Determining when students are able to use school or personal electronic devices for educational purposes.
3. Supervising students' use of electronic devices.
4. Responding effectively to disciplinary issues from inappropriate electronic device usage.
5. Communicating appropriately with administrators, parents, and students if the MoE policy is violated from electronic device usage.

SECTION 5 DEVICE USAGE

PART A: Privacy

The Ministry of Education will usually not interfere with an individual's technology use, as long as no activity violates policy, law or compromises the safety and well-being of the school community. However, the Ministry of Education reserves the right to monitor and regulate activities that take place using Ministry-owned technology or any devices connected to the school network.

Further, the MoE reserves the right to investigate any reports of inappropriate actions related to any technology used at school. In response to reports of unauthorised use of technology, the Ministry of Education reserves the right to inspect all emails and messages sent through the school's network or accessed on a school computer, any files saved onto Ministry owned technology, or under school-based accounts. Further, web browsing on school grounds may be monitored. Individuals should have a limited expectation of privacy when using both Ministry owned and personal technology on school property or at school events. The Ministry of Education may install software and/or hardware to monitor and record all IT resources usage, including email and Web site visits. The Ministry retains the right to record or inspect any and all files stored on MoE owned systems.

Staff are advised that serious disciplinary action up to and including termination of employment may result from evidence of prohibited activity obtained through monitoring or inspection of electronic messages, files, or electronic storage devices. Illegal activity involving technology resource usage may be referred to appropriate authorities for prosecution.

PART B: Expectations for Technology Use

The use of education sector technology resources is a privilege granted to employees for the enhancement of job-related functions. All Ministry owned technologies, the school network, and its Internet connection are intended primarily for educational purposes. Educational purposes include academic research and collaboration, classroom activities, career development, communication with experts, and a variety of other activities.

Electronic devices brought to school shall be restricted to educational and administrative purposes in approved locations and times. Authorised users shall:

1. Use electronic devices in accordance with the expectations set forth in school procedures and MoESKN policies.
2. Comply with the guidelines set by the school administration for the use of electronic devices while on school property or while engaged in a school-sponsored activity.
3. Access the school network using approved infrastructure only.

Employees may have limited access to technology resources for personal use if they comply with the provisions of this policy. Recreational use of the school network and other technologies are

permitted, unless those activities are prohibited elsewhere in this policy, or in cases where the activity interferes with any educational or operational process of the school, students or other teachers.

Personal Use of the Internet

Employees may have limited access to technology resources for personal use, if they comply with the provisions of this procedural directive. Occasional and incidental personal use of the MoE technology resources, and Internet access is allowed subject to limitations.

Personal use of the internet is prohibited if:

- It materially interferes with the use of technology resources by the MoE.
- It burdens the MoE with additional costs.
- It's use interferes with the staff member's employment duties or other obligations to the MoE.
- Such personal use includes any activity that is prohibited under any MoE procedural directive.

Infractions related to personal use may result in the revocation of this privilege. Employees may also face disciplinary action up to and including termination, civil litigation, and/or criminal prosecution for misuse of these resources. The MoESKN is not responsible for any damages, injuries, and claims resulting from infractions of this policy.

Digital Management

Devices are preconfigured for deployment in a MoE mobile device management environment. Any attempt to gain administrative privileges to alter/remove any MoE-installed configuration is strictly prohibited.

Downloads, File Storage, and Sharing

All users are expected to maintain copies of school and work-related files in cloud-based or hardware storage. The MoE has deployed the Microsoft M365 cloud and desktop platforms, which provide users with free, 1 terabyte (1TB) cloud storage of content. Therefore, the use of Microsoft's free services are strongly recommended to avoid the loss of content.

The MoE is not responsible for the loss of files on damaged or missing computers. Downloaded media files of a personal nature should not be stored on school-provided local or cloud storage. The MoE reserves the right to review, restrict or remove personal content, and to limit certain device functionality.

Internet Access and Data Security

Users may not reveal any personal information about themselves or other students, staff, or the administration, such as name, phone number, address, passwords, etc. through any means of digital

communication on a school-owned device. This includes email and internet web sites, as well as social media, such as Facebook, Twitter, Snapchat, iMessage, etc.

Social Networking and Web Publishing Technologies

While on a school campus, access to social networking websites, photo-sharing websites, messaging tools, and online publishing such as blogging, and website creation tools may be controlled by Internet filtering technology or may require the express permission of a school administrator. Social networking sites may be permitted based on grade-level appropriateness and instructional relevance. In such instances users may utilize these tools, and digital social connections for responsible academic collaboration and sharing.

Recording, Video, and Photography

No identifiable photographs, video or other media of any person, including staff, may be published on the internet, stored on the device, or used in print without appropriate written consent. All media recordings (audio, video, typed, etc.) require prior written permission from all parties being recorded. Appropriate written consent for any minor student is defined as a signature by a parent or legal guardian of the student. Any student appearing in captured photos or video may not be identified by name.

Cell Phones, Portable Game Devices, and other Mobile Devices

Mobile apps such as calculator, camera, voice-recorder, and an unlimited number of other communications and collaborative apps available on many smart phones may have educational relevance and may be utilized in a responsible manner.

PART C: Unauthorised Use of Electronic Devices

General

Prohibited uses of electronic devices includes, but are not limited to:

1. Areas where there is a reasonable expectation of privacy, such as changing rooms or toilets.
2. Circumventing school's approved network infrastructure to access internet connections using an external wireless provider.
3. Downloading files that are unrelated to job responsibilities and activities.
4. Engaging in non-educational activities such as playing games, watching videos, using social media, listening to music, texting, or taking personal calls.
5. Accessing information that is confidential.
6. Obtaining unauthorised access and using it to alter, destroy, or remove data.
7. Engaging in cyberbullying which involves using technology to harass, threaten, embarrass, or target another person.
8. Infecting a device with a virus or other program designed to alter, damage, or destroy.
9. Infringing upon copyright laws or plagiarising protected information.

10. Using network resources for commercial or party-political purposes.
11. Committing a crime under local statues.
12. Users may not alter, change, modify, repair, or reconfigure settings on school-owned devices without the express prior permission of school technology staff.
13. Users may not purposefully spread or facilitate the spread of a computer virus or other harmful computer program or alter settings on school-owned technology in such a way that the virus protection software or other security measures would be disabled.
14. Users may not attempt to utilise password hacking utilities to acquire passwords.
15. Accessing secured files, resources, or administrative areas of the school network without express permission or the proper authority.

All employees who have access to or may have access to personally identifiable student records shall adhere to all standards included in the code of conduct, and other applicable laws and regulations, related to the release of student information.

Respect for the Privacy of Others

Staff shall not use technology resources to reveal confidential or sensitive information, student data, or any other information covered by existing privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms. Staff who engage in the unauthorized release of confidential information via MoESKN technology resources will be subject to sanctions in existing policies and procedures associated with unauthorized release of such information.

Schools are communities and community members must respect the privacy of others.

- Users may not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to others.
- Users may not misrepresent or falsely assume the identity of others.
- Users may not re-post information that was received privately without the permission of the sender/owner of the information.
- Users may not post private information about others.
- Users may not use another person's account.
- In circumstances where a staff member has been given another user's account with special privileges, that account may not be used outside of the terms under which it was given.

Inappropriate Communications

Inappropriate communication is prohibited in any public messages, private messages, and material posted online by staff. Inappropriate communication includes, but is not limited to the following:

- Obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language or images typed, posted, or spoken by staff.
- Information that could cause damage to an individual or the school community or create the danger of disruption to the school environment.
- Personal attacks, including prejudicial or discriminatory attacks.

- Harassment (persistently acting in a manner that distresses or annoys another person) or stalking of others.
- Knowingly or recklessly posting false or defamatory information about a person or organization.
- Communication that promotes the destruction of property, including the acquisition or creation of weapons or other destructive devices.

Staff may not engage in any form of cyber-bullying, i.e., using any technology to harass, insult, antagonize, slander, demean, humiliate, intimidate, embarrass, or annoy others. Cyber-bullying in any form is unacceptable and will not be tolerated. Any cyber-bullying, on or off-campus, that is determined to substantially disrupt the safety and/or well-being of a person or the school is subject to disciplinary action.

Offensive Material

Users may not access material that is offensive, profane, or obscene including pornography and hate literature. Hate literature is anything written with the intention to degrade, intimidate, incite violence, or incite prejudicial action against an individual or a group based on race, ethnicity, nationality, gender, gender identity, age, religion, sexual orientation, disability, language, political views, socioeconomic class, occupation, or appearance (such as height, weight, and hair color).

Staff shall not access, store, display, distribute, edit, or record sexually explicit or extremist material using MoE technology resources. The incidental and unsolicited receipt of sexually explicit or extremist material, such as might be received through email, shall not constitute a violation of this section, provided that the material is promptly deleted and neither stored nor forwarded to other parties. If a staff member accidentally accesses or receives obscene, pornographic or otherwise offensive material, he/she is to immediately notify their school administrator so that such material can be traced and/or blocked from further access. This is not merely a request; it is an obligation.

Spam

Spamming can occur through emails, instant messages, or text messages. Staff may not post or send chain letters or spam. Staff shall not be punished if prohibited materials are forwarded to the Technology Department to alert them that material has been received. Examples of this material include, but are not limited to, SPAM and phishing emails.

Commercial Use

Commercial use of school technology is prohibited. Staff may not use school technology to sell, purchase, or barter any products or services. Staff may not resell school-supplied network resources to others, including, but not limited to, network/Internet access, and disk storage space.

Political Use

Political use of school technology is prohibited without prior, specific permission from the Head of School. Staff may not use school technology to campaign for or against, fundraise for, endorse, support, critise or otherwise be involved with political candidates, campaigns or causes.

Digital management of Software and Apps

Staff shall not download executable software, including freeware and shareware, unless it is required to complete their job responsibilities. Staff shall not upload or otherwise transfer out of the Ministry of Education's direct control any software licensed to the MoE or data owned or licensed by the MoE without explicit written authorization.

Staff shall not use MoE technology resources to intentionally disable or overload any computer system or network, or to circumvent any system intended to protect the privacy or security of the MoE's technology resources. Unauthorized access to the Internet is prohibited from any device that is attached to any part of the school's network.

Intellectual Property and Plagiarism

Users should not post or make accessible to others the intellectual property; including, but not limited to text, photographs, and video; of someone other than him/herself. This includes intellectual property that staff were given permission to use personally, but not publicly. This behavior constitutes copyright infringement. Staff may not configure a school computer or personally owned computer to transmit or receive copyrighted material, or to engage in any illegal file sharing.

Plagiarism is unacceptable and will not be tolerated. All staff are expected to model academic honesty.

SECTION 7 CONSEQUENCES OF VIOLATION OF POLICY

Part A: Response to Policy Violations

The use of school-owned technology devices and networks, on school property or at school events, is a privilege not a right. This privilege comes with personal responsibility; where an individual fails to act responsibly with their use of technology, the privilege of that use may be suspended and/or revoked.

Individuals who do not comply with this Policy will be subject to appropriate consequences. Consequences may include, but are not limited to, the following, either singularly or in combination depending on the individual circumstances:

- temporary confiscation of device.
- Search of device contents to locate evidence of misuse.

- Suspension, and/or revocation of access privileges to personal and school technology resources, for instances:

    - Use of the network(s)/computers only under direct supervision
    - Suspension of network privileges
    - Revocation of network privileges
    - Suspension of computer privileges
    - Revocation of computer privileges
    - Suspension of email account
    - Revocation of email account

Disciplinary Action

Individuals violating this policy May be be subject to disciplinary actions as outlined in the Public Service Code of Discipline, 2014. The Ministry of Education cooperates fully with local authorities in any investigations related to illegal activities conducted on school property at school sponsored events or through education sector technologies.

SECTION 6 PROCEDURES

Part A: Device Repair and Replacement

Device Repair

All device repairs are coordinated by the MoE in accordance with device warranties. If a user suspects their device might have an issue, it is not the user's responsibility to attempt to repair the device. At the first sign of any issue, hardware-related or software-related, it is the user's obligation to contact the school administration. Any attempt to repair a device could result in a voided warranty and a charge for the device.

If the device becomes inoperable due to a system error, the MoE will make every effort to provide a spare device for use while the device is being repaired or replaced. The terms of the technology policy also apply to the substitute computer.

School personnel shall not provide repair or replacement for user-owned electronic devices. The school and school personnel shall not be responsible for any negative consequences to electronic devices caused by running specific software or by accessing the school network.

Device Replacement

If the first and subsequent issued device is damaged, the user may choose to pay charges for an additional device. If the user chooses this option, the additional charge will be US$550. The user may also choose to provide their own device to with the approval of the MoE.

Charging cords, power adapters and carrying cases are issued with all devices. If an individual loses or damages a charging cord or power adapter, the user may choose to pay charges for a

replacement. The charge for replacement power cords/adapters is US$40. The user may also choose to provide their own compatible charging device with the approval of the MoE.

Devices and related equipment issued may be collected periodically for the purpose of maintenance and upgrade, at which time a thorough inspection will occur. Any visible issues, damage, or missing parts will be noted. Charges may be assessed for replacement of missing components and/or any excessive damages that hinder use of the device.

Lost and Stolen Devices

Users are solely responsible for the care and use of personal electronic devices they choose to bring to school. Users bringing these devices to school do so at their own risk. The Ministry of Education and school personnel shall not be liable for the loss, damage, misuse, or theft of any student-owned electronic device possessed or used during the school day while on school property or in school buildings, vehicles, or contracted vehicles, during transport to and from school, while attending school-sponsored activities.

If a Ministry issued device or related equipment is lost or stolen on school property, the user must immediately report this to the school administrator. If the device or related equipment is stolen when away from school property a police report should be filed, and the school administration must be advised of the theft and the police report. The MoE is not responsible for stolen devices. If the device is not recovered, the cost of a replacement device will be assessed.

SECTION 7 ACKNOWLEDGEMENT AND AGREEMENT

Paste Device Acceptance Form