THE MINISTRY OF EDUCATION,
YOUTH & INFORMATION

BYOD

BRING YOUR OWN DEVICE
POLICY
FOR SCHOOLS

SEPTEMBER 2020

Every Child Can Learn
Every Child Must Learn

TABLE OF CONTENTS

BRING YOUR OWN DEVICE (BYOD) FOR LEARNING POLICY

INTRODUCTION

Technology impacts everything we do in our daily lives. It is without a doubt that there are significant gains to be realised by embracing technology and its application to instructional design and delivery. Globally, educators have developed innovative approaches to the integration of new and existing technologies in the classroom with the sole objective of enhancing the student learning experience.

In 2014, the Ministry of Science, Energy and Technology (MSET) through the e-Learning Jamaica Company (e-LJam) collaborated with the Ministry of Education, Youth & Information (MoEYI) to implement the Tablets in Schools (TIS) pilot project. This initiative was established with the objective of improving the educational levels of Jamaicans in an effort to stimulate a fully connected and knowledge-based society. The lessons learnt from the TIS pilot project was used to inform the Tablet in Infant and Primary Schools (TIIPS) initiative that will see the roll out of tablets to infant and primary schools in 2020.

Despite the significant gains realized by the TIS initiative, it is concluded that the continued provision by the Government of Jamaica (GoJ) of one-to-one devices to students is unsustainable. As a result, in addition to providing select institutions with class set (s) to use in a shared manner, the MoEYI seeks to explore the possibility of a **Bring Your Own Device (BYOD)** approach for Jamaica's education sector.

For the purposes of this Policy, BYOD refers to the permitted use of an approved private portable computing device (for example, a laptop, tablet, smartphone etc.) by a student at school or on the school's network in furtherance of the student's learning. Access to the School Network may be at no cost to students and their families. Students participating in a BYOD programme can use their own devices (BYO Devices) as an alternative to, or as an additional level of support to devices provided by the Government/school (Class set Devices). Learning activities utilizing BYO devices can take place both on-line, typically by connecting to the school's network; or off-line, for example, utilizing materials that have been downloaded to the BYO Device.

The MoEYI is aware that some schools have already begun to implement aspects of a BYOD approach to support the demand by students and teachers for the use of **Information Communication Technologies (ICTs)** in the teaching learning process. These initiatives range from informal or *ad hoc* use by some teachers to a strictly controlled whole-school approach.

The concept of 'mobile learning' has come into sharp focus with the declaration by the World Health Organization (WHO) of the Coronavirus disease (COVID-19) Pandemic on March 10, 2020. Countries across the world including Jamaica responded by closing all schools, among other social distancing measures meant to control the spread of the Virus. In order to ensure that learning continues in the face of physical school closures, may schools resorted to utilizing various distance education modalities, including on-line learning. This latest development has seen a surge in the number of children joining the online world for the first time to support their studies and maintain social interaction.

When schools do re-open, it is anticipated that mixed modalities of instruction will be needed to ensure adherence to prevailing public health requirements. As we look to the future, it is clear that education as we know it in our school system will undergo a paradigm shift - one in which ICT enabled learning can no longer be considered optional.

Based on the foregoing, there is now an urgent need for coherent policy direction from the MoEYI to guide the adoption of the BYOD approach in Jamaica's school system. Consequently, this document contains the national framework that will govern the BYOD approach for learning for implementation in all schools**.**

This Policy is organized in seven (7) sections as follows:

Section 1. Policy Framework

Section 2. Evaluating School Readiness to Introduce BYOD

Section 3. Approved Devices & Institution Requirements

Section 4. General Guidelines for Acceptable Use

Section 5. Consequences for Disruption and Misuse

Section 6. Institution Liability

Section 7. Stakeholder Roles and Responsibilities

A Glossary of technical terminology (Page 18) is included at the end of the Policy. Also included are templates for a School BOYD Agreement (containing an Acceptable Use Policy), which may be used or modified to reflect each school's circumstances (Appendix I). Finally, the MoEYI's Child Online Protection (COP) Protocols is contained in Appendix II.

SECTION 1 - POLICY FRAMEWORK

AIM

1.1 This BYOD policy provides the background, rationale and general guidelines for schools (early childhood to secondary school level) seeking to implement a BYOD programme. The BYOD policy is intended to work in conjunction with school-based policies and procedures. The policy guidelines will support schools, to enable students to bring their own technology and devices to school solely for the purpose of enhancing the learning process.

GUIDING PRINCIPLES

1.2 The guiding principles of the BYOD Policy are:

- Security and Safety
- Inclusion and Participation
- Sustainability – Learning for the future

OBJECTIVES

1.3 The objectives of the BYOD Policy are to:

- Transform the ways in which teachers deliver their lessons by creating an educational system in which facilitators use ICTs in the teaching and learning environment to encourage learning and improve students' performance while effectively managing of the learning process.
- Transform the learning process by integrating ICTs within the curriculum and during assessments, encourage critical thinking, problem-solving, decision making and digital citizenship inclusive of the values inherent in collaborating and communicating through the integration of ICTs in the education system.

LINKAGES WITH OTHER POLICIES

1.4 The policy supports the United National Sustainable Development Goals, and in particular to ensure inclusive and equitable quality education and promote lifelong learning opportunities for all.

1.5 The Policy was developed to align with the standards for students outlined in the 2016 International Society for Technology in Education (ISTE) which highlight the following critical attributes for a 21st- century student:

- Empowered Learner
- Responsible Digital Citizen
- Knowledge Constructor
- Innovative Designer
- Computational Thinker
- Creative Communicator
- Global Collaborator

1.6 Additionally, the Policy is aligned with recent guidance provided by the International Telecommunications Union (ITU) for CPO, which aims to provide a safe, age-appropriate, inclusive and participatory digital space for children and young people.

1.7 Nationally, the Policy supports Jamaica's National Development Plan, Vision 2030, and in particular, Goal 1: Jamaicans are Empowered to Reach their Fullest Potential which is aligned to National Outcome 2: World-Class Education and Training; and National Outcome 11: A Technology-Enabled Society.

1.8 The Policy is consistent with national policies and legislation to promote a modern ICT framework. Sector-wise, the Policy is aligned to proposals being pursued by the Ministry under its draft ICT in Education Policy, the goals of which are:

- learning opportunities for all
- transforming the Teaching and Learning Process
- efficient management and administration of the Education System
- promoting the development of ICT Innovations.

SECTION 2 – SCHOOL READINESS TO INTRODUCE BYOD

2.1 This section recognizes that each school's situation is unique. The benefits and challenges of introducing BOYD to the school must be carefully considered and consultation undertaken before a decision is made. Implementing a BYOD approach to learning is a school-based decision that must be undertaken **in consultation with and supported by the MoEYI and stakeholders**.

WHY BYOD?

2.2 Research has shown that the use of portable computing devices such as tablets and laptops can enhance the teaching the learning process. For example, it can support student-centred learning where students assume greater responsibility for their own learning. In turn, student self-directed and active learning can lead to higher levels of motivation and engagement by students. Additionally, the use of devices facilitates differentiated instruction within classes in which students can engage with class activities at their own pace, using their personal approach.

2.3 A BYOD programme can enhance these benefits having regard to the following:

- By enabling students who have access to a BYO Device, the school can more effectively allocate Class Set Devices to students who need them, thereby maximizing student participation in ICT-enabled learning.
- Students may prefer to use technology and devices with which they are familiar, and a BYOD programme allows them to do so for educational purposes.
- Students are more likely to take proper care of their personal property.

POTENTIAL CHALLENGES OF BYOD

2.4 Examples of some of the potential challenges that schools may identify in their planning process are:

- worries about human resource capacity and additional workload
- worries about infrastructural capacity and the risk to security of the school's network
- ensuring equitable access by students to educational technology
- concerns about student safety on-line

2.5 Assisted by MoEYI, some of the key questions to be considered by the school in the BYOD planning stage are set out in the table below.

Broadband	Devices and Device Management
• Type of broadband connection available? • Total broadband currently available? • Option to upgrade? • Strategies for sharing connection and bandwidth?	• Types of devices to be allowed (see Section 3)? • Total number of devices expected? • Device management processes and systems needed (See Section 4)?

Wi-Fi Network	Network Use
• Wi-Fi infrastructure currently installed? • Use and performance of current Wi-Fi? • Who will do sit survey/network optimisation? • Requirements indicated by site survey • Type/capacity of existing and required Access Points? • Positioning of new Access Points	• Where and when will devices be used? • How often will devices be used?? • Amount of video streaming expected • Amount of data uploading expected?
IT Support	**Access Control**
• What IT support will students be offered? • What will be handled in school/region? • Training required? • What services can be outsourced?	• How will user identity be authenticated? • Device screening and authentication methods? • What services/applications/materials can users access? • Will access to some applications be restricted?
	Safeguarding
	• Content filtering strategies and tools (See Appendix 2)? • How will acceptable use policy be developed (See Section 3)

Adapted from: "BYOD for Schools: Technical advice for school leaders and IT administrators", http://www.eun.org/documents/411753/817341/BYOD_Technical_guide_full_v7.pdf

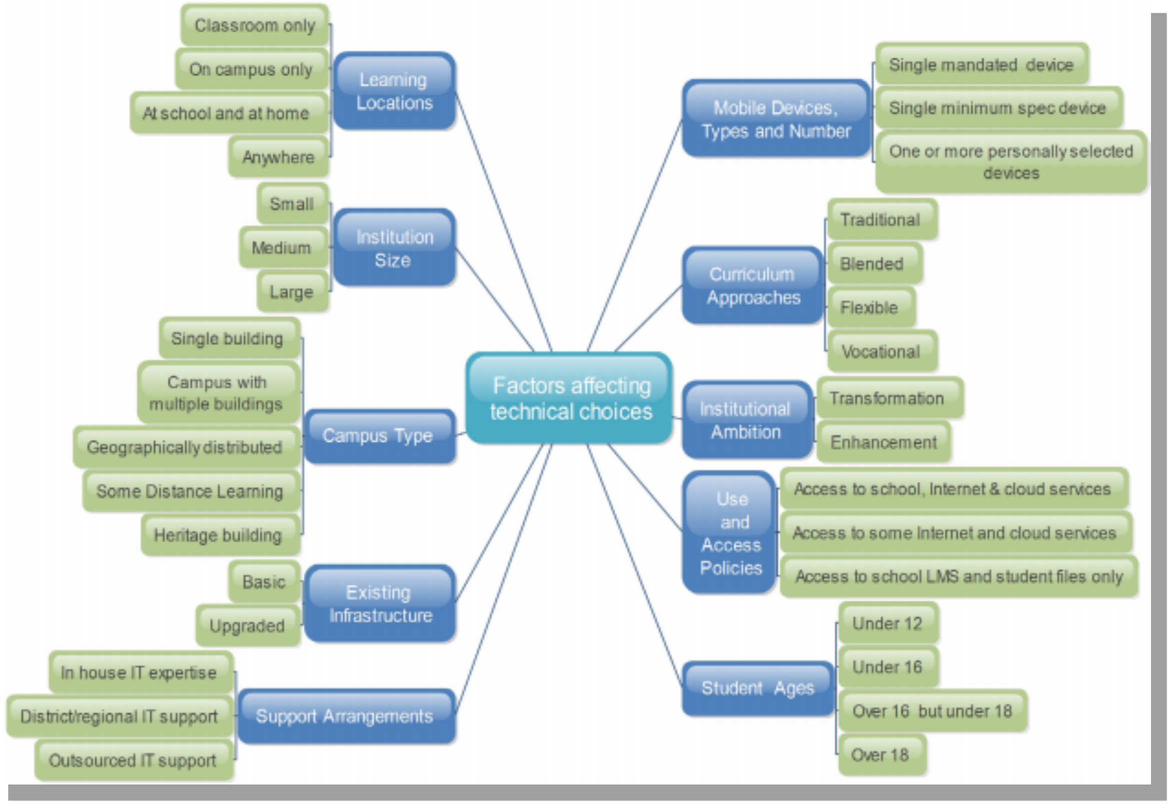
SECTION 3 – APPROVED DEVICES AND INSTITUTION REQUIREMENTS

APPROVED DEVICE REQUIREMENTS:

3.1 Stipulating technical specifications for BYO Devices ensures that all students have the same or similar devices and therefore learning experience. Standardization has both pedagogical and technical benefits, making the work of teachers easier and simplifying IT support. Upon the completion of a comprehensive and careful evaluation (See Section 2), schools may recommend specific devices for use in the enhancement of the learning process. These devices may include:

- laptops
- netbooks
- tablet computers
- mobile phones
- virtual and augmented reality headsets

3.2 The recommendation of approved devices should take into consideration the suitability of the device for educational enrichment, and all aspects of the device's technical specifications such as make, model, operating systems, storage, screen size, and processor. The diagram below illustrates some of the factors affecting approved BYO Device requirements.



Source: http://www.eun.org/documents/411753/817341/BYOD_Technical_guide_full_v7.pdf

3.3 For the preparation of use, all BYO Devices should be fully charged before school each day and have its software (Operating System and Antivirus and Malware Protection Software) updated when necessary.

SCHOOL INFRASTRUCTURE REQUIREMENTS:

3.4 Each school is required to have the necessary infrastructure which will facilitate a stable power supply from the local grid. A stable power supply is critical to the functioning of equipment such as wireless routers, hubs, and local file servers.

3.5 All schools will be required to establish appropriate **Wireless Local Area Networks (WLAN)** with designated **WI-FI Hotspots**. Each Hotspot will facilitate **Role-Based Access Control** protocols. Students, teachers, and school administrators may be given designated usernames and passwords which will provide network access in accordance with the limits and rights assigned to each group.

3.6 Each school is required to ensure adequate cyber security measures are in place to:

- protect the school network from unauthorized access and other risks; and
- safeguard students from inappropriate content and communication. A COP Protocol (Appendix 2) has been developed by the MoEYI and must be adhered by all schools.

SCHOOL HUMAN RESOURCE REQUIREMENTS:

3.7 Teachers and select faculty members must be sufficiently trained in relation to the following:

- new approaches relating to BYOD classroom management strategies.
- providing basic in-class technical support to students.
- technical support in relation to student device and school WLAN functionality.

SECTION 4 – GENERAL GUIDELINES FOR ACCEPTABLE USE

This section addresses the stakeholder code of conduct, and development of stakeholders as responsible digital citizens.

GUIDELINES FOR THE CLASS SETTING:

4.1 Class teachers may invite students to bring BYO Devices to class, on designated days and for specific educational purposes in accordance with the School's BYOD Policy. BYO Devices, as opposed to Class Set Devices where they exist, are not to be utilized for general use by students. Opportunities for use of BYO Devices may vary from class to class based on units of study, appropriateness of certain tools, age, and experience of students.

4.2 The use of personal devices in classrooms should be carefully planned, guided, and supported by teachers. Such use may include:

- carrying out online research
- creation of multimedia content such as videos, audio etc.
- commenting on blogs
- adding content to websites
- participating in online discussions
- word processing

4.3 Each teacher has the discretion to allow and regulate the use of BYOD in the classroom and on specific projects.

4.4 Teachers should adhere to staff polices governing interaction with students, particularly outside of scheduled classes/activities and when using social media, messaging apps and email.

GUIDELINES FOR STUDENTS AND FAMILIES

4.5 Students and **parents** participating in the BYOD programme must adhere to the school's BYOD Policy, BYOD Agreement and/or Acceptable Use Policy (AUP). A BYOD Agreement Template, containing an AUP, is appended to this Policy (Appendix 1) and can be used or modified by schools to support their own situation. This or other similar Agreements must be read, signed, and returned to the school office as a condition for participating in the BYOD programme.

PERMITTED USE

4.6 The primary use of BYO Devices at school or on the school's network is for educational purposes. Use of BYO Devices at school or on the school's network should therefore be limited to support classroom instructional delivery and other approved school activities. For these purposes, student may use the School wireless network and content **Filtered** broadband. Use of other unfiltered public wireless connections, such as mobile networks, is not allowed during school hours. Students should only access digital content on websites which are relevant to the classroom curriculum.

4.7 BYO Devices brought onto school grounds should be labelled for identification and logged in daily and given a unique reference number. BYO Devices should be charged prior to school and run on battery power while at school. Charging of BYO devices on school property may be permitted in the sole discretion of authorized school personnel. BYO Devices should be kept in silent mode while on school premises unless authorised by a teacher. Headphones may be used with the permission of a teacher. Permission should be sought before attaching any school property to a BYO Device. If a BYOD Device has a camera and/or video capability, these must be disabled whilst at school or during school hours, unless the capability is genuinely required in connection with authorized learning activities. This ensures that the privacy of the user and other students is not inadvertently breached by the capture and dissemination of images.

PROHIBITED USE

4.8 BYO devices should not be used as an aid in the dishonest completion of exams, assignments, or quizzes. Students should not use BYO Devices to record, transmit, or post photographic images or video of a person or persons on campus during school hours or during school activities unless authorised by a teacher.

4.9 Students and Parents/Guardians must be made aware and acknowledge that the school's network filters will be applied to a BYO device's connection to the internet and any attempt to bypass the network filters is prohibited. The school's BYOD Agreement and/or AUP should prohibit students from:

- brining a device on premises that infects the network with a **Virus**, **Trojan**, or program designed to damage, alter, destroy, or provide access to unauthorized data or information; and
- altering, **hacking** or attempting to bypass the school's network security systems.

NO EXPECTATION OF PRIVACY

4.9.1 It is also important for students and parents to acknowledge and accept that the use of a BYO Device on the School's network or while at School is not private. The BYO Agreement and/or AUP should provide that the school may, without prior notice, log, supervise, access, view, monitor, and record use of student devices on the school's network or while on school campus at any time for any reason related to the operation of the school.

4.9.2 The BYOD Agreement and/or AUP should provide that devices may be subject to search and temporary seizure by school administrators where it is reasonably suspected that a violation of the following has occurred:

- school's Student Code of Conduct or Student Handbook
- school's BYOD Policy, BYOD Agreement and/or school's AUP
- any relevant law or regulations

MONITORING SOFTWARE

4.9.3 The MoEYI supports the use of **Monitoring Software** to ensure COP and adherence to the school's BYOD Policy, BYOD Agreement and/or AUP. The school's BYOD Agreement should specify that schools may use monitoring software to enable the viewing of the screens and activity on BYO devices while on the school's network or on school premises.

SECTION 5 – CONSEQUENCES FOR DISRUPTION AND MISUSE

5 Existing Student Codes of Conduct and Student Handbooks should be revised to ensure provision is made for actions to be taken against students who breach the school's BYOD

Policy, BYOD Agreement and/or AUP as appropriate in the circumstances. Recommended actions based on severity and number of breaches include:

- parents notified of the breach.
- BYO Device taken away for a stipulated period.
- BYO Device taken away and kept in the administrative office until a parent collects it.
- Restrictions in participation in BYOD programme
- Temporary or permanent exclusion from the BYOD Programme

SECTION 6 – SCHOOL LIABILITY STATEMENT

6 Students bring their own devices to school at their own risk. It is the duty of the students to be responsible for the upkeep and protection of BYO Devices, including the use of protective/carrying cases and up-to-date anti-virus and malware protection software. The school's BYOD Agreement should clearly stipulate that the school is not liable for:

- BYO Devices that are damaged while at school or during school-sponsored activities.
- BYO Devices that are lost or stolen at school or during school-sponsored activities.
- maintenance or upkeep of any BYO Device (keeping it charged, installing updates or upgrades, fixing any software or hardware issues).

SECTION 7 – STAKEHOLDER ROLES AND RESPONSIBILITES

7 To ensure sustainability and guarantee the success of the BYOD programme it is imperative that all stakeholders understand and accept their roles and responsibilities.

A. **The Ministry of Education Youth & Information** is responsible for:

- developing, monitoring, evaluating, and reviewing the BOYD Policy to ensure a flexible and user-friendly national framework which supports the implementation of effective BYOD programmes in schools.

- consulting with the Information Communications Technology Authority (the ICTA) on the applicability of any directives, codes, standards, and guidelines issued by the ICTA that may be relevant to the BYOD Policy framework.

- ensuring schools adhere to the BYOD Policy framework in their implementation of school BYOD programmes, particularly the principles of inclusion and participation, to ensure that students and families who wish to take part in a BYOD programme are not confronted with unrealistic expectations.

- ensuring that schools are familiar with any ICTA directives, codes, standards and guidelines and adhere to them.
- ensuring that schools plan for the use of BYOD in the classroom to support learning.
- support schools and families to plan for the creation of a safe and empowering on-line environment for children, including the identification of keys risks and harms for children on-line and the development of effective measures for child online protection.
  providing students on government supported programmes such as PATH access to devices for educational use.

B. **MoEYI & e-LJam** are responsible for:

- providing technical support for Class Set Devices purchased by the GoJ and managed by the MoEYI for student use.
- providing support with wireless connection technical issues, such as to ensure that all student devices can readily connect to the school's network.

C. **The Boards of Management (School Boards) of Schools** are responsible for:

- in consultation with the MoEYI, overseeing the implementation and operation of the school's BYOD programme and for this purpose, appointing a BYOD School Board committee or delegating the responsibility of BYOD to an existing School Board committee.
- ensuring engagement with various stakeholders represented on the School Board prior to and throughout the implementation of a BYOD programme in the school.
- critically reviewing and approving school-based BYOD policies and procedures, including the School's BYOD Policy, the BYOD Agreement and or /AUP, revisions to staff and student codes of conduct and/or Handbooks, and other associated procedures and documents.

D. **Principals and other school administrators** are responsible for:

- ensuring engagement with parents and staff, through their School Associations, prior to the implementation of a

BYOD programme in the school and throughout its operation.

- developing standard operating procedures for approval by the School Board to govern the school's BYOD programme, including the school's BYOD Policy, BYOD Agreement and/or AUP
- ensuring the MoEYI's COP Protocols are in place.
- revising school polices to include student codes of conduct, student handbooks, staff policies, complaints procedures and child protection reporting procedures for approval of the School Board to ensure that these policies and procedures address assessed risks associated with implementing a BYOD programme.
- ensuring the school provides the necessary ICT infrastructure including wireless access points that support student devices connecting to the school's Wi-Fi network.
- conforming with any ICTA directives, codes, standards and guidelines and co-operating with any ICTA authorized ICT audit.
- including the BYOD approach for learning in educational planning and teacher and staff professional learning activities.
- registering BYO Devices and assigning usernames and passwords after receiving duly signed BYOD Agreement and/or AUP or similar documentation.
- offering parents, guardians and teachers support to better understand online risks and harms for students, for example, by providing Tips on online safety.

E. **Teachers** are responsible for:

- providing guidance for use of ICT within the classroom and associated learning environments, including ensuring students understand and follow the school's BYOD Policy, BYOD Agreement and/or AUP and associated procedures and documents.
- delivering curriculum and learning activities that use technology to build knowledge, understanding and produce outcomes that are not possible or practical without the use of technology.

- ensuring the technology available to all students is considered when developing curriculum and learning activities.

- planning for the use of a BYOD approach to learning in the classroom through the National Standards Curriculum (NSC).

- ensuring that Cyber Safety is a key component of ICT based teaching and learning and that the MoEYI's COP Protocols are observed.

- ensuring that all interaction with students outside of scheduled classes/activities for example *via* social media platforms, messaging apps or emails, is in strict compliance with the school's policies and procedures.

F. **Parents** are responsible for:

- accepting that the sole use of BYO Devices at school or on the school's network is for educational purposes. Further, that approval to connect any BYO Device to the school network is at the discretion of the school principal.

- reading, signing, and returning the school's BYOD Agreement and/or AUP or similar document to the school office at least once per year.

- ensuring that the appropriate use of BYO Devices and being 'cyber safe' is discussed regularly with their child.

- ensuring their child understands his or her roles and responsibilities as a responsible digital citizen when accessing and using the school's ICT facilities and is aware of and adheres to the terms of the school's BYOD Policy, BYOD Agreement and/or AUP or similar documents.

- monitoring and supporting their child's use of BYO Devices so that they can fully benefit for the opportunities that the digital environment offers while being protected for online risks and harms for children.

- ensuring the maintenance and upkeep of BYO Devices, including but not limited to the use of parental control settings, age-appropriate protective gear and that up-to-date anti-virus and malware protection software is installed on the device.

G. **Students** are responsible for

- reading, signing, and returning the school's BYOD Agreement and/or AUP or similar document to the school office at least once per year.
- Adhering to the terms of the school's BYOD Policy, BYOD Agreement and/or AUP and associated procedures and documents by demonstrating appropriate and lawful behaviour when accessing and using the school ICT facilities and BYO Devices.
- Maintaining a school user-name and password security.
- Maintaining BYO Device password security.
- Adhering to requirements in any MoEYI or school social media policies, procedures and guidelines.
- Ensuring that while at school, their BYO Device is stored in a reasonably safe place during school hours, in line with any specific arrangements made by the school.

SECTION 8 – MONITORING AND EVALUATION

8 The implementation of the BYOD policy will be monitored to gauge the level of inclusion of the instruments into the teaching and learning activities. However, the BYOD policy will be reviewed after three (3) years to assess its impact.

ACRONYMS

AUP	Acceptable Use Policy
BYOD	Bring Your Own Device
COP	Child Online Protection
e-LJam	E-Learning Jamaica Company
ICT	Information Communication Technology
ICTA	Information Communication Technology Authority
MoEYI	Ministry of Education Youth and Information
MSET	Ministry of Science, Energy and Technology
TIS	Tablets in Schools
TIIPS	Tablets in Infant and Primary Schools
WHO	World Health Organization
WLAN	Wireless Local Area Network

GLOSSARY

Bring Your Own Device (BYOD): BYOD refers to the permitted use of an approved private portable computing device by a student at school or on the school's network in furtherance of the student's learning. Students participating in a BYOD programme can use their own devices (BYO Devices) as an alternative to, or as an additional level of support to devices provided by the Government/school (Class set Devices). Learning activities utilizing BYO devices can take place both on-line, typically by connecting to the school's network; or off-line, for example, utilizing materials that have been downloaded to the BYO Device. Approved BYO Devices may include but are not limited to smart phones, laptops, tablet PC or net books.

Information Communication Technologies (ICT): means any technology employed in the collection, storage use or transmission of information, and includes any technology that involves the use of computers or any telecommunication system.

Parent(s): includes guardian(s) or other person(s) having the care and control of a child.

Platform: refers to an underlying computer system on which application programmes can run (Windows, Mac OS, Android).

Hack/Hacking: generally refers to unauthorized intrusion into a computer or a network. The person engaged in hacking activities is known as a hacker. This hacker may alter system or security features to accomplish a goal that differs from the original purpose of the system. Hacking can also refer to non-malicious activities, usually involving unusual or improvised alterations to equipment or processes.

WLAN: A wireless local area network (WLAN) is a wireless distribution method for two or more devices that use high-frequency radio waves and often include an access point to the Internet. A WLAN allows users to move around the coverage area, often a home or small office, while maintaining a network connection.

Hotspot: A hotspot is a specific location that provides Internet access via a WLAN. The term is generally synonymous with a Wi-Fi connection.

Monitoring Software: Monitoring software observes and tracks the operations and activities of users, applications and network services on a computer or enterprise systems. This type of software provides a way to supervise the overall processes that are performed on a computing system and provides reporting services to the system or network administrator. Monitoring software is also known as computer surveillance software.

Role-based access control (RBAC): is a method of access security that is based on a person’s role within a business. Role-based access control is a way to provide security because it only allows employees to access the information they need to do their jobs while preventing them from accessing additional information that is not relevant to them. An employee's role determines the permissions he or she is granted and ensures that lower level employees are not able to access sensitive information or perform high-level tasks.

Website/Network Filter: A website filter is a network application/utility used for website control and/or traffic management. Website filters are used as tools, procedures, and security features to block network traffic according to a user or network preferences. Website filters are built into devices or software including routers, switches, firewalls, anti-spyware software, and browsers. A website filter is configured by a network administrator. By default, most website filters block Web pages prone to spyware, viruses, pornography, fraud, etc.

Virus: A virus is a type of malicious software (malware) comprised of small pieces of code attached to legitimate programs. When that program runs, the virus runs.

Trojan/Trojan Horse: A Trojan horse is a seemingly benign program that when activated, causes harm to a computer system. A Trojan horse is also known as a Trojan virus or Trojan.

Phishing: Phishing is the fraudulent act of acquiring private and sensitive information, such as credit card numbers, personal identification and account usernames and passwords.

Spyware: Spyware is infiltration software that secretly monitors unsuspecting users. It can enable a hacker to obtain sensitive information, such as passwords, from the user's computer.

APPENDIX I

FORM 1

BRING YOUR OWN DEVICE (BYOD) AGREEMENT AND ACCEPTABLE USE POLICY (AUP) FOR POST-PRIMARY EDUCATIONAL INSTITUTIONS

(This Template combines a BYOD Agreement and AUP and can be used or modified by post primary schools to support their own situations)

Purpose

The purpose of this Agreement and AUP is to set out certain standards which apply when students are permitted to use their own devices for authorized educational purposes at [school name] (the School). The terms of this Agreement and AUP affects all persons who are subject to and or take the benefit of the school's BYOD Programme. Parents/guardians and students must read, sign, and return this Agreement and AUP to the school office at least once in every school year as a pre-condition to participating in the School's BYOD Programme. By doing so, parents/guardians and students acknowledge and accept the terms and conditions of this Agreement and AUP as applicable to them and agree to abide by them.

This Agreement and AUP should be read in conjunction with other relevant school polices, including the [School BYOD Policy], [the Student Code of Conduct], [the Student Handbook], [name other policies].

Definitions

Access:Internet connectivity through the School's wireless infrastructure.

Agreement and AUP: means this BYOD Agreement and Acceptable Use Policy.

BYO Device: refers to a student's privately-owned portable computing device such as a laptop, tablet, netbook or smartphone, that is approved for use under the School's BYOD programme.

BYOD Policy means the BYOD Policy approved by this School in keeping with the Ministry's BYOD Policy for Learning.

Bring Your Own Device (BYOD): BYOD refers to the permitted use of an approved private portable computing device (for example, a laptop, tablet, smartphone etc.) by a student at school or on the school's network in furtherance of the student's learning.

the Ministry means the Ministry of Education, Youth, and Information.

Network: includes wired and wireless technology networks provided to the School and the Schools' local area networks (LAN).

School: means this School.

School Administrator: includes any Grade Supervisor, Vice Principal or Principal.

Student: means a person enrolled as a student of the School.

School Declaration:
The School supports the use of technology for the purpose of enhancing and supporting teaching and learning. The School has decided to allow students to use their own portable computing devices to access the School's Networks and to use their devices at School to aid in students' learning subject to the terms of this Agreement/AUP. Access to the School Network may be at no cost to students and their families. In partnership with the Ministry and other governmental departments and agencies, the School is dedicated to providing access by appropriate technology and devices that will improve the potential of our students. We envision a learning environment where technology is a seamless tool in teaching and learning process.

IMPORTANT NOTICE for Students and parents: The use of BYO Devices on the School Network and at School during school hours is a privilege, not a right and is accompanied by very stringent responsibilities. Allowing students to bring and use their BYO devices presents both opportunities and risks, which must be managed appropriately. The Principal shall have overall responsibility for the operation for this Agreement and AUP. However, it is the responsibility of Parents/Guardians/Students participating in the BYOD programme to comply with the terms of this Agreement and AUP at all times, act in a responsible manner, and obey the directions of teachers and school administrators.

Students who do not comply with this Agreement and AUP will be subject to measures stipulated in this Agreement and AUP. This may include (temporary) confiscation of the BYO Device, restricted Access, temporary or permanent loss of Access, or temporary or permanent exclusion from the BYOD Programme. If the breach arises from a deliberate or negligent disregard of any of the requirements of this Agreement and AUP, this may, in the absolute direction of the School, result in disciplinary action against the Student under the Student Code of Conduct and/or Student Handbook, or legal action as necessary.

Students will be held accountable for their actions and are encouraged to report any accidental unauthorized use immediately to the class teacher or any School Administrator.

Students must respect and protect their privacy and that of others by*:*

- using their own assigned accounts and no other account.
- only using their passwords and no other password.
- not disclosing their password to others.
- only accessing authorized data or networks.
- avoiding distribution of private information/graphic or audio-visual materials about others or themselves.

Students must respect and protect the integrity, availability, and security of all electronic resources by*:*

- observing all school internet filters and posted network security practices.
- reporting security risks or violations to a class teacher or School Administrator.

- not destroying or damaging data, network infrastructure, or other resources that are critical to the proper functioning of the School's Network or other BYO Device users.
- conserving, protecting, and sharing these resources with other users of the School's Network or BYOD Programme.
- notifying a class teacher or School Administrator of BYO Device or Network malfunctions immediately.

Students must respect and protect the intellectual property of others by:

- following copyright laws (such as not making illegal copies of music, games, or movies).
- citing sources when using the work of other persons (not plagiarising).
- being ethical at all time with the use of the BYO Device.

Students must respect and practice the School's BYOD principles by:

- communicating only in ways that are kind and respectful.
- reporting threatening or discomforting materials to a class teacher or School Administrator.
- not intentionally accessing, transmitting, copying, or creating material that violates this Agreement and AUP, the School's BYOD Policy, Student Code of Conduct and or Student Handbook (such as messages/content that are pornographic, threatening, rude, discriminatory, or meant to harass).
- not intentionally accessing, transmitting, copying, or creating material that is illegal (such as obscenity, stolen materials, or illegal copies of copyrighted works) or otherwise knowingly use the BYO Device in a manner that could constitute an offence under any relevant statute.
- Avoiding spam sites, chain letters, or other mass unsolicited mailings.
- Not buying, selling, advertising, or otherwise conducting business, unless approved as a school project.
- Avoiding the use of social networking sites, during school hours and/or when connected to a School's Network, unless it is for educational purposes and is directed by a classroom teacher or approved by a School Administrator.

Students can use the BYO Device to do the following*:*

- design and post web pages, apps, and other material from school resources.
- communicate electronically via tools such as email, chat, text, or video calls (students require a class teacher's permission).
- use the resources for any educational purpose.

Supervision and monitoring

IMPORTANT NOTICE to parents and students: The use of BYO Devices while at School or when accessing the School's Network is not private. As part of its measures to help manage the risks associated with a BYOD programme, the School supervises and monitors the use of all BYO devices through the teachers or any other authorized personnel for compliance with this Agreement and AUP. The monitoring team is vested with the right to examine, use and disclose any data found on a BYO Device or the School's Network in order to advance the health, safety, discipline, or security of any student or other person, or to protect the School's Network, property of the School and others. They may also use this information in evidence for disciplinary actions and will furnish evidence of crime to the Police.

The School is the sole determinant of which uses constitute acceptable use and to limit access to such uses.

Activities that warrant immediate action by Teachers and School Administrators.

Activities that:

- create a security and/or safety risk to staff, students, and visitors of the School.
- cause harm to others (including emotional and mental harm) or damage School or personal property.
- use profane, abusive, threatening, or harassing language or images.
- make damaging or false statements about others or accessing, transmitting, or downloading offensive, harassing, or disparaging materials.
- Delete, copy, modify, or forge other Students' names, emails, files or data, disguising one's identity, impersonating other users, or sending anonymous email.
- Advertise; promote sites for social and commercial efforts and events or otherwise use websites, email, networks, or other technology for personal gain.
- Take photos/videos of other individuals without their consent.
- Intentionally access, create, store or transmit material that may be deemed to be offensive, indecent, obscene, intimidating, or hostile; or that harasses, insults or attacks others.
- Are in violation all copyright laws.
- Use the BYO Devices or the School's Network for non-academic related bandwidth activities such as non-educational games or transmission of large audio/video files or serving as a host for such activities.
- Any other activity that may warrant the immediate action of the School

Approved Requirements for BYO Device.

Standardization of BYOD requirements has both pedagogical and technical benefits. Stipulating technical specifications for BYO Devices ensures that all students have the same or similar devices and therefore learning experience. The recommended technical specifications are:

Device Type	**Tablet devices with keyboard attached (can be detachable)**
Screen Size	**7-10 inches**
Operating System	**Android KK4**
Wi-Fi Adaptor	**802.11 N or AC capable**
Battery Life	**Minimum 6 hours**
Warranty/insurance coverage	**Extended Warranty with Accidental Damage**

The School will not be able to support devices on BYO programme that do not comply with the following minimum specifications.

Device Type	**Smartphone/ Phablet/similar smart device**
Screen Size	**6-9 inches**
Operating System	**Android**
Wi-Fi Adaptor	**802.11 N or AC capable**
Battery Life	**Minimum 6 hours**
Warranty/insurance coverage	**Extended Warranty with Accidental Damage**

Personal gaming devices are not allowed under the BYOD programme. The School decides on the type of allowed device.

School Liability Statement:

IMPORTANT NOTICE to parents/guardians/students: Students bring BYO devices to use at School or on the School network at their own risk. Students are expected to act responsibly with regards to their BYO device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices. This includes protective/carry cases and exercising caution when storing the device. The School or the Ministry is in no way responsible for:

- BYO Devices that are broken while at School or during school-sponsored activities
- BYO Devices that are lost or stolen at School or during school-sponsored activities
- Maintenance or upkeep of any BYO Device (keeping it charged, installing updates or upgrades, anti-virus and malware protection software, fixing any software or hardware issues).
- Costs of any data/phone calls incurred.

The School and the Ministry make no warranty or representation as to the quality of the School's Network, internet connection or power supply. The School reserves the right at any time and for any purpose to limit Student Access to its Network to timed sessions or otherwise.

Condition for the registration and use of BYOD Devices

- The privately owned device must meet the approved technical requirements for the School's BYOD programme (see table) and be registered as a BYO Device with the School.
- BYOD Devices must be made available to the authorized personnel for the installation of the necessary security and/or client software.
- Parents/guardians and students seeking to participate in the School's BYOD programme must sign this Agreement/AUP at least once in every school year.
- Students participating in the School's BYOD programme must adhere to the terms of this Agreement/ AUP.
- Students must report promptly any suspected or observed security breach.
- BYO Devices must be clearly labelled for identification purposes. The labels should not be easily removable.

- Students should not attach any school-owned equipment to their BYO Devices without the permission of the class teacher or School Administrator.
- BYO Devices must be fully charged before bringing them to School or class.
- BYO Devices must have a supported operating system and current anti-virus and malware protection software installed on the device. Students must continue to maintain the latest service updates. All software on BYO Devices must be legally and appropriately licensed.
- To avoid accidental use, BYO Device camera and video capabilities must be switched off unless authorized by the class teacher for instructional use.
- The BYO Device must be in silent mode unless otherwise instructed by a class teacher. The use of headphones may be permitted with the permission of a class teacher.
- The Student is to follow the instructions of the class teacher in the use of the BYO Device.

BYOD Device Details: ______________________________ (eg., Tablet – include manufacturer, type of device here)

As a student I understand and will abide by this Agreement and AUP. I understand that any violation of this Agreement and AUP may result in not being able to use my portable device in School and could mean other disciplinary action.

Student Name: ____ (in capitals)

Student's Age: __________________________Student's Grade/Form: _______________________

Student signature: _____________________________________ Date: ________________________

As Parent/Guardian I understand that my child accepts the responsibilities outlined in this Agreement and AUP. I have discussed the Agreement and AUP with them and we both understand own responsibilities.

Authorizing Parent/Guardian Name: ____(in capitals)

Authorizing Parent/Guardian signature: ______________________________________ Date: _____

FORM 2

BRING YOUR OWN DEVICE (BYOD) AGREEMENT AND ACCEPTABLE USE POLICY (AUP) FOR [NAME] INFANT AND PRIMARY SCHOOL (THE SCHOOL)

(This Template combines a BYOD Agreement and AUP and can be used or modified by infant and primary schools to support their own situations)

Purpose: The School's bring your own device (BYOD) programme involves allowing students to bring their own portable computing devices to school to support learning activities in accordance with the terms of this BYOD Agreement and AUP. Access to the School Network may be at no cost to students and their families. In an effort to support student centered learning and allow students to take more control of their own learning, the School will allow students to use certain privately-owned portable computing devices in School or to access the School's network. Students and parents wishing to participate in the BYOD programme must accept the responsibilities stated in this BYOD Agreement and Acceptable Use Policy (AUP) as outlined below, and must read, sign, and return this form to the school office once every school year.

Types of devices allowed under this policy: For the purpose of this program, a 'BYOD Device' refers to a privately-owned portable computing device (as opposed to a school/government device or 'Class Set Device') which the student is permitted to use such as a tablet, laptop, netbook, or suitable smart phone. Standardization of BYOD requirements has both educational and technical benefits. Stipulating technical specifications for BYOD Devices ensures that all students have the same or similar devices and therefore learning experience. The recommended technical specifications are:

Device Type	Tablet devices with keyboard attached (can be detachable)
Screen Size	7-10 inches
Operating System	Android KK4
Wi-Fi Adaptor	802.11 N or AC capable
Battery Life	Minimum 6 hours
Warranty/insurance coverage	Extended Warranty with Accidental Damage

The School will not be able to support devices on BYOD programme that do not comply with the following minimum specifications.

Device Type	Smartphone/ Phablet/similar smart device
Screen Size	6-9 inches
Operating System	Android
Wi-Fi Adaptor	802.11 N or AC capable
Battery Life	Minimum 6 hours
Warranty/insurance coverage	Extended Warranty with Accidental Damage

Personal gaming devices are not allowed under the BYOD programme. The school decides on the type of allowed device.

BYOD Acceptable Use Policy (AUP):

1. Any student who wishes to use a privately owned portable computing device at school or to access the School's network must read and sign this Agreement and AUP.
2. A parent /guardian of the student must also read, sign and submit the Agreement and AUP to the school office.
3. **IMPORTANT NOTICE: Use of BYOD Devices on the School Network and while at school is not private.** The School reserves the right to inspect or monitor BYOD Devices during school hours.
4. During school hours students are allowed to use their device for learning related activities only.
5. Students will comply with teachers' requests regarding use of BYOD devices during school hours, and classes.
6. BYOD devices must be charged prior to bringing them to School so as to be usable during school hours. Charging devices in the School is not an option.
7. Students may not use the devices to record, transmit or post photos or video of other teachers or students. No images or video recorded at school can be transmitted or posted at any time without the permission of their teachers. To avoid accidental use, camera and video capabilities must be switched off.
8. The BYOD Device must be in silent mode unless otherwise instructed by a class teacher. The use of headphones may be permitted with the permission of a class teacher.
9. Student may use the School wireless network and content filtered broadband. Use of other unfiltered public wireless connections, such as mobile networks, is not allowed during school hours.
10. Violations of any School policies or rules involving a BYOD Device may result in a student not being allowed to continue using the device during school hours and/or disciplinary action, for a period to be determined by the School.
11. The School reserves the right to change this Agreement and AUP in line with overall school policies as approved by the Board of Management of the School from time to time.

School Liability Statement:

IMPORTANT NOTICE to parents/guardians/students: Students bring their devices to use at School or on the School network at their own risk. Students are expected to act responsibly with regards to their own device, keeping it up to date and as secure as possible. It is their duty to be responsible for the upkeep and protection of their devices. This includes protective/carry cases and exercising caution when storing the device. The School or the Ministry of Education, Youth and Information is in no way responsible for:

- BYOD Devices that are broken while at School or during school-sponsored activities
- BYOD devices that are lost or stolen at School or during school-sponsored activities
- Maintenance or upkeep of any BYOD Device (keeping it charged, installing updates or upgrades, anti-virus and malware protection software, fixing any software or hardware issues).
- Costs of any data/phone calls incurred.

The School and the Ministry make no warranty or representation as to the quality of the School's Network, internet connection or power supply. The School reserves the right at any time and for any purpose to limit Student Access to its Network to timed sessions or otherwise.

BYOD Details: _____________________________ (eg., Tablet – include manufacturer, type of device here)

As Parent/Guardian I understand that my child accepts the responsibilities outlined in this Agreement and AUP. I have discussed the Agreement and AUP with them and we both understand our responsibilities.

Authorizing Parent/Guardian Name: ____________________________(in capitals)

Authorizing Parent/Guardian signature: _________________________Date: _____

As a student/on behalf of student (as appropriate in discretion of school), I understand and will abide by this Agreement and AUP. I understand that any violation of this Agreement and AUP may result in not being able to use my/student's portable device in School and could mean other disciplinary action.

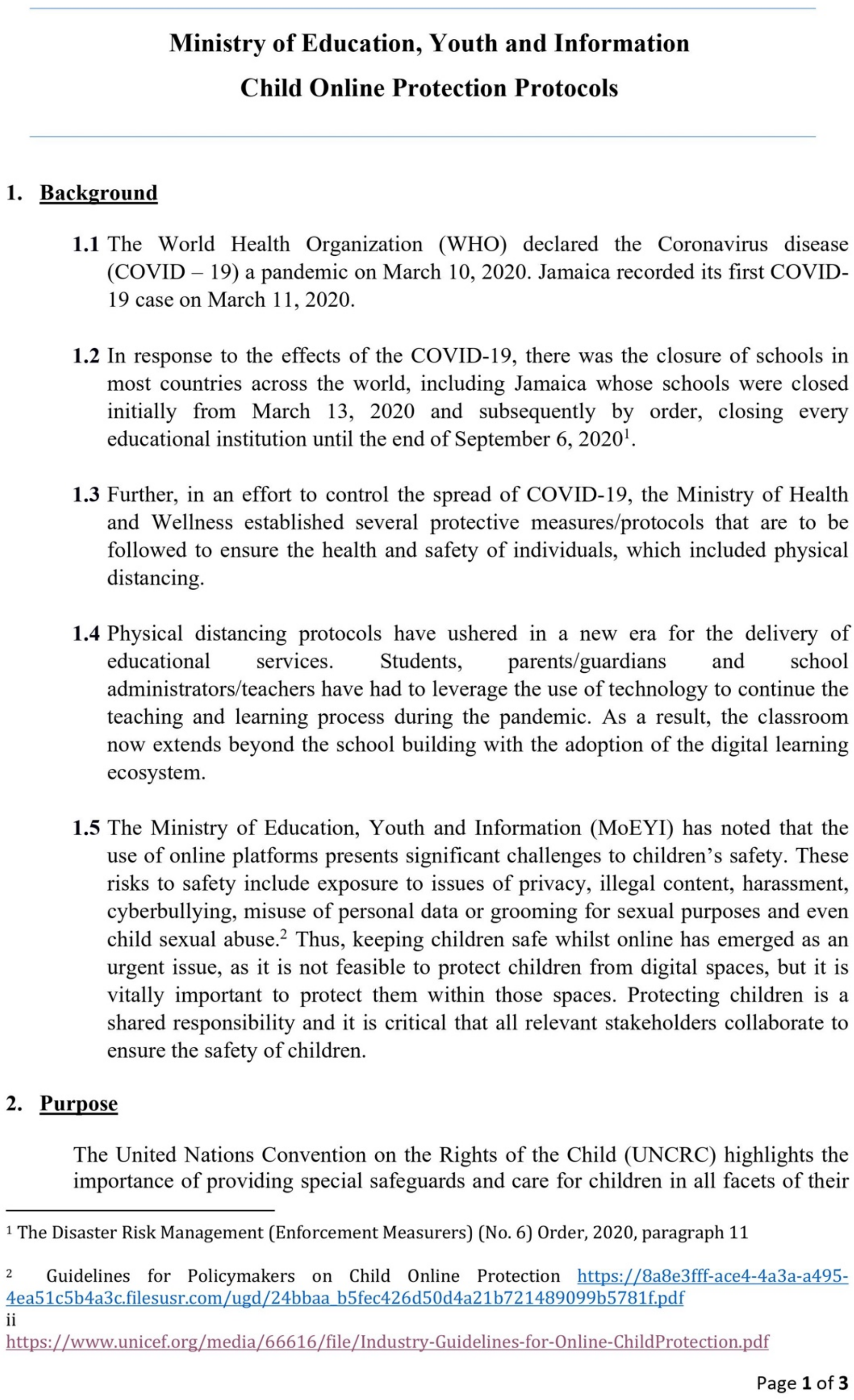
Student Name: ____(in capitals)

Student Age: ____________________________Student's Grade:______________

Student signature /for and on behalf: __________________Date: _____________

APPENDIX II

CHILD ONLINE PROTECTION (COP) PROTOCOLS



Ministry of Education, Youth and Information
Child Online Protection Protocols

1. <u>Background</u>

1.1 The World Health Organization (WHO) declared the Coronavirus disease (COVID – 19) a pandemic on March 10, 2020. Jamaica recorded its first COVID-19 case on March 11, 2020.

1.2 In response to the effects of the COVID-19, there was the closure of schools in most countries across the world, including Jamaica whose schools were closed initially from March 13, 2020 and subsequently by order, closing every educational institution until the end of September 6, 2020[1].

1.3 Further, in an effort to control the spread of COVID-19, the Ministry of Health and Wellness established several protective measures/protocols that are to be followed to ensure the health and safety of individuals, which included physical distancing.

1.4 Physical distancing protocols have ushered in a new era for the delivery of educational services. Students, parents/guardians and school administrators/teachers have had to leverage the use of technology to continue the teaching and learning process during the pandemic. As a result, the classroom now extends beyond the school building with the adoption of the digital learning ecosystem.

1.5 The Ministry of Education, Youth and Information (MoEYI) has noted that the use of online platforms presents significant challenges to children's safety. These risks to safety include exposure to issues of privacy, illegal content, harassment, cyberbullying, misuse of personal data or grooming for sexual purposes and even child sexual abuse.[2] Thus, keeping children safe whilst online has emerged as an urgent issue, as it is not feasible to protect children from digital spaces, but it is vitally important to protect them within those spaces. Protecting children is a shared responsibility and it is critical that all relevant stakeholders collaborate to ensure the safety of children.

2. <u>Purpose</u>

The United Nations Convention on the Rights of the Child (UNCRC) highlights the importance of providing special safeguards and care for children in all facets of their

[1] The Disaster Risk Management (Enforcement Measurers) (No. 6) Order, 2020, paragraph 11

[2] Guidelines for Policymakers on Child Online Protection https://8a8e3fff-ace4-4a3a-a495-4ea51c5b4a3c.filesusr.com/ugd/24bbaa_b5fec426d50d4a21b721489099b5781f.pdf
ii
https://www.unicef.org/media/66616/file/Industry-Guidelines-for-Online-ChildProtection.pdf

lives. The international community and local stakeholders are in agreement as to the need to ensure that digital spaces are safe for children to learn, play and participate. The MoEYI's *Child Online Protection Protocols (hereinafter "the Protocols") w*ill support students, school administrators/teachers and parents/guardians in enabling safe navigation of the digital environment. The focus of the *Protocols* is on providing the appropriate guidelines to ensure that children have the best possible opportunity to leverage the use of online services whilst mitigating the risks which arise therefrom.

3. Protocols

3.1. The best interests of the child should be a primary consideration in designing, developing, recommending or facilitating any online service or digital platform for use by a child.

3.2. Antivirus and malware protection software is to be installed on all devices being used and is to be kept up to date. Parents whose child/children will participate in their schools' BYOD programme must ensure that the appropriate protection software is installed on their child/children's devices. The MoEYI must ensure appropriate protection software is installed on those devices that it has procured for students on PATH.

3.3. Devices being used are to be password protected (with strong password) and locked when not in use or logged off/signed out.

3.4. Appropriate web content filtering tools and solutions are to be employed to protect students from harmful or inappropriate content. This should form a part of the Monitoring team to be established by schools.

3.5. A plan is to be made for making and securing data backups (offsite) at determined levels of frequency to enable disaster recovery and provide options in the event of cyber-attacks or other crises.

3.6. An incident response plan is to be prepared to provide instructions to help detect, respond to, and recover from network security incidents, which might include cybercrime, data loss, and service outages that threaten daily work. The School in conjunction with the PTA should agree on the development of such a plan.

3.7. Reliable and secure Wi-Fi connectivity is to be provided by the school for use by students across school campuses, particularly in classrooms and libraries.

3.8. Ensure access to remedy by making available grievance and reporting mechanisms for any child rights violation or any online safety risk; and for concerns reported to be addressed, with timely provision of information about the status of the report.

3.9. A specific individual and/or a Monitoring Team is to be designated with responsibility for child online protection. This individual/team should have access to the necessary internal and external stakeholders; and should be provided with the authority to take the lead in raising the profile of child online protection across the school. The individual/team should employ appropriate strategies to obtain ongoing feedback on the child online safety mechanisms implemented.

3.10. The school's position on acceptable use of, and the consequences of breaches or misuse of its devices or services is to be explicitly stated in easily understood language. Emphasis should be placed on what behaviour is and is not acceptable, and is particularly geared for children and their parents/guardians. Schools should bring to the parent's attention the Acceptable Use Policy in its BYOD Policy

3.11. Age-appropriate digital literacy training is to be provided to help children to learn the how to stay safe online. Training is to include a focus on prevention of and protection from cyberbullying. This could be part of the training and sensitisation that school should provide for parents and students

3.12. Educate parents on how to become involved in their children's online activities. For example, providing parents with the ability to review children's privacy settings; and help to build parents' abilities to support and speak with their children about being responsible digital citizens. This could form part of the training and sensitization agenda of the National Parenting Support Commission, the National Parent/Teachers Association of Jamaica, Schools Parenting Teachers Association as well as parents educating themselves.

3.13. The Ministry of Education, Youth and Information to provide information on appropriate tools and solutions to monitor student's online activity to help keep them safe. Children are to be made aware that their activities online are being monitored prior to the use of such tools.

REFERENCES:

Bring Your Own Technology Procedures (n.d.). In Tasmanian Government Department of Education - Document Centre. *Retrieved from https://documentcentre.education.tas.gov.au/Documents/Bring%20Your%20Own%20Technology%20%20Procedures.pdf*

Guidance document for the provision of wireless network installations in primary schools (2016). In Department of Education and Skills, Ireland - .

Guidance document for the provision of wireless network installations in post primary schools (2017). In Department of Education and Skills, Ireland -

International Society for Technology in Education (ISTE). (n.d.). ISTE STANDARDS FOR STUDENTS. In *http://www.iste.org/docs/Standards-Resources/iste-standards_students-2016_onesheet_final.pdf?sfvrsn=0.23432948779836327*. Retrieved September 21, 2017.

k12 Blueprint*. (n.d.). BYOD Readiness Checklist for School Teachers. In k12 Blueprint. Retrieved October 22, 2017, from https://www.k12blueprint.com/sites/default/files/BYOD-Checklist-Teachers.pdf*

Lambton Kent District School Board. (n.d.). ADMINISTRATIVE PROCEDURES*. In Lambton Kent District School Board. Retrieved February 14, 2018, from http://www.lkdsb.net/Board/PoliciesRegulations/Documents/Bring%20Your%20Own%20Device%20(BYOD)%2 0Administrative%20Procedures.pdf*

Techopedia, Techopedia.com, *https://www.techopedia.com/dictionary. Accessed 10 Apr. 2018.*

PREPARED BY THE MINISTRY OF EDUCATION,
YOUTH & INFORMATION