File: IIBJ-A
(Replaces: IIBJ)

Norton Public Schools
BRING YOUR OWN DEVICE (BYOD) Policy

Purpose

The Norton Public School District is committed to moving toward a 21st century learning environment. As part of this commitment, the district will allow access to our academic wireless network for students and staff using their own technology. Students and staff members will be able to access a filtered Internet connection to be used for educational purposes. We want all members of the school community to embrace appropriate use of technology so that they may have access to global resources when and where needed.

Users will be responsible for adhering to all other district/building acceptable use policies, codes of conduct, or administrative guidelines while using the district's wireless network. Students and staff members who do not accept the Norton Public Schools BYOD Agreement will not be permitted network access using personally owned devices. The use of devices by students is not permissible unless teacher or staff member approval has been granted.

Definition of "Device"

For the purpose of this B.Y.O.D. program, "device" means any privately owned wireless communication or portable electronic equipment. This includes, but is not limited to: smartphones, tablets, netbooks, laptops, iOS devices, chromebooks and e-readers.

Internet

When using personal devices on school grounds for educational purposes, only the Wi-Fi provided by the school may be accessed. This is in accordance with the Children's Internet Protection Act (CIPA). The **Children's Internet Protection Act** (**CIPA**) requires that K-12 schools and libraries in the United States use Internet filters and implement other measures to protect children from harmful online content as a condition for the receipt of eRate funding.

Security and Damages

- Responsibility to keep personal technology secure rests with the individual owner.
- The district is NOT responsible for stolen or damaged personal technological devices.
- The district is NOT responsible for the maintenance or repair of any personal technology.
- The district is NOT responsible for any costs incurred due to use of personal technology.
- The district's network filters will be applied to all connections to the Internet and attempts will not be made to bypass the filters.

- The district technology staff will advise only for troubleshooting purposes regarding issues on personal technological devices.
- Infecting the network with a virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information is in violation of this policy.
- Processing or accessing information on school property related to “hacking”, altering, or bypassing network security policies is in violation of this policy.
- The district has the right to collect and examine any device that is suspected of interfering with the network, or is the source of an attack or virus infection.

Illegal Uses/Consequences--Students, Employees, Visitors

Chapter 272, Section 99C of the Massachusetts General Law states in part that it is illegal for someone to attempt to or actually record any communication secretly or to procure another to do so. This is a felony, punishable by a state prison term of up to five years and or a fine of not more than $10,000.00. Some states have laws that allow for “one-party” consent, whereby so long as one party involved in the recording is aware of it and consents to it, others do not have to be aware of it. This is not the case in Massachusetts. Anyone recorded must be aware of it and must consent to it. In addition to the criminal penalties a violator might face, there are also potential civil damages that could be pursued by a victim.

Student or Staff Member Name:_____

Student or Staff Member Signature: _____

Parent/Guardian Signature: _____
(required if student is under 18 years old)

Date: _____

Adopted: February 23, 2015