TECHNOLOGY RESPONSIBLE USE

The Board intends for students and employees to benefit from technological resources while remaining within the bounds of safe, legal and responsible use. Accordingly, the Board establishes this policy to govern student and employee use of school district technological resources. This policy applies regardless of whether such use occurs on or off school district property, and it applies to all district technological resources, including but not limited to computer networks and connections, the resources, tools and learning environments made available by or on the networks, and all devices that connect to those networks.

A. EXPECTATIONS FOR USE OF DISTRICT TECHNOLOGICAL RESOURCES

School district technological resources may only be used by students, staff and others expressly authorized by the District. The use of district technological resources, including access to the internet, is a privilege, not a right. Individual users of the district's technological resources are responsible for their behavior and communications when using those resources. Responsible use of district technological resources is use that is ethical, respectful, academically honest and supportive of student learning. Each user has the responsibility to respect others in the school community and on the internet. Users are expected to always abide by the generally accepted rules of network etiquette and to apply the rules of good Digital Citizenship. General student and employee behavior standards, including those prescribed in applicable Board policies, the Student Code of Conduct, and other regulations and school rules, apply to use of the internet and other district technological resources.

In addition, anyone who uses district computers or electronic devices or who accesses the school network or the internet using district resources must comply with the additional rules for responsible use listed in the Dorchester School District Two Modern Learning Device Handbook. These rules are intended to clarify expectations for conduct but should not be construed as all-inclusive. Prior to receiving a district issued device and access to the district network, all students and staff must complete the district's acceptable use policy orientation.

All students and employees must be informed annually of the requirements of this policy and the methods by which they may obtain a copy of this policy. Before using district technological resources, students and employees must sign a statement indicating they understand and will strictly comply with these requirements. Students and employees will acknowledge awareness that the district uses systems to monitor and detect inappropriate use of technological resources. Failure to adhere to these requirements will result in disciplinary action, which may include revocation of user privileges. Willful misuse may result in disciplinary action and/or criminal prosecution under applicable state and federal law.

B. RULES FOR USE OF SCHOOL TECHNOLOGICAL RESOURCES

1. District technological resources are installed and maintained by members of the Technology Department. Students and employees shall not attempt to perform any installation or maintenance without the permission of the Technology Department.

2. Under no circumstance may software purchased by the district be copied for personal use.

3. Students and employees must comply with all applicable laws, including those relating to copyrights and trademarks, confidential information, and public records. Any use that violates state or federal law is strictly prohibited. Plagiarism of internet resources will be treated in the same manner as any other incidents of plagiarism, as stated in the Student Code of Conduct.

4. Users of district technological resources, including a person sending or receiving electronic communications, may not engage in creating, intentionally viewing, accessing, downloading, displaying, storing, printing or transmitting images, graphics (including still or moving pictures), sound files, text files, documents, messages or other material that is obscene, defamatory, profane, pornographic, harassing, violent or promoting violence including the manufacturing or purchasing of weapons, demeaning or promoting hatred against another person or group of persons with regard to race, color, sex, religion, national origin, age, marital status, disability, genetics, or handicap, abusive or considered to be harmful to minors. Users may not post chain letters or engage in spamming. All users must comply with all applicable Board policies, the Student Code of Conduct, Modern Learning Device Handbook, and the Employee Handbook.

5. Users may not use the device for commercial purposes, which include but are not limited to offering, providing, or purchasing products or services.

6. Users may not use the device for political lobbying, expression of political ideas, or promoting political campaigns or candidates.

7. Users may not install or use any internet-based file sharing program designed to facilitate sharing of copyrighted material, without the permission of the

Superintendent or designee.

8. Users of district technological resources may not send electronic communications fraudulently (i.e., by misrepresenting the identity of the sender).

9. Users must respect the privacy of others. When using email, social media, or other forms of electronic communication, users must not reveal personally identifying information or information that is private or confidential, such as the home address or telephone number, credit or checking account information or social security number of others. In addition, users must not disclose personally identifying, private, or confidential information concerning others on district websites or elsewhere on the internet, including social media sites and applications, without the written permission of a parent or guardian or an eligible student, except as otherwise permitted by the Family Educational Rights and Privacy Act (FERPA). Users may not forward or post personal communications without the author's prior consent.

10. Users may not intentionally or negligently damage computers, computer systems, electronic devices, software, computer networks, or data of any user connected to district technological resources. Users may not knowingly or negligently transmit computer viruses, malware, or self-replicating messages or deliberately try to degrade or disrupt system performance.

11. Users may not create or introduce games, network communications programs, or any foreign program or software onto any district computer, electronic device, or network without the express permission of the Superintendent or designee.

12. Users are prohibited from engaging in unauthorized or unlawful activities, such as hacking, using unauthorized proxies to circumvent the filtering system, or using the computer network to gain or attempt to gain unauthorized or unlawful access to other computers, computer systems, or accounts.

13. Users should not share usernames and passwords with others. Users are prohibited from using another individual's ID or password for any unauthorized purpose.

14. Employees may not use passwords or user IDs for any data system (e.g., the state student information and instructional improvement system applications, time-keeping software, etc.), for an unauthorized or improper purpose. Students may not modify any password without the express consent of the district.

15. If a user identifies a security problem on a technological resource, he or she must immediately notify a system administrator. Users must not share the problem with other users. Any user identified as a security risk may be denied access.

16. Staff connection of personal mobile devices to the district's network is permitted while the user is on the premises but such use will not be supported by the District. The Board is not responsible for the content accessed by users who connect to the internet via their personal technology.

17. It is the responsibility of the user to back up data and other important files regularly.

18. Those who use district owned and maintained technologies to access the internet at home are responsible for both the cost and configuration of such use.

19. Students who are issued district owned and maintained devices must also follow these guidelines as outlined in the Modern Learning Device Handbook.

C. RESTRICTED MATERIAL ON THE INTERNET

The Internet and electronic communications offer fluid environments in which users may access or be exposed to materials and information from diverse and rapidly changing sources. The Board recognizes it is impossible to predict with certainty what information on the Internet users may access or obtain. Nevertheless, district personnel will take reasonable precautions to prevent students from accessing material and information that is obscene, pornographic or otherwise harmful to minors, including violence, nudity, or graphic language that does not serve a legitimate pedagogical purpose according to the Children's Internet Protection Act (CIPA). It is the responsibility of the user to not seek out information which is obscene, pornographic, or otherwise harmful to minors. Additionally, users may not take any action which is intended to circumvent any district placed filters or to conceal any actions executed on the device.

The Board recognizes parents of minors are responsible for setting and conveying the standards their children should follow when using media and information sources when students use their device outside of school. The district maintains the right to filter the content that can be accessed on district-owned devices at all times, including when the device is being used off campus and outside of school hours. Nonetheless, the District is not responsible for information accessed independently by the student or any other person.

Any district staff or computer technicians who discover sexually explicit images of apparent minors must report this to school administration and local law enforcement. The report must include the name and address of the person in possession of the computer or to whom the computer is assigned. Failure of any district employee to properly notify law enforcement of discovered child pornography on district technology will result in disciplinary and possible legal action.

D. PRIVACY

Students, employees, visitors and other users have no expectation of privacy in anything they create, store, send, delete, receive, or display when using the District's network, devices, internet access, email system, or other technological resources owned or issued by the district, whether the resources are used at school or elsewhere, and even if the use is for personal purposes. The district may, without notice, (1) monitor, track and/or log network access, communications and use; (2) monitor and allocate fileserver space; and (3) access, review, copy, store, delete or disclose the content of all user files regardless of medium, the content of electronic mailboxes and system outputs, such as printouts, at any time and for any reason. Such purposes may include, but are not limited to, maintaining system integrity, security or functionality, ensuring compliance with Board policy and applicable laws and regulations, protecting the district from liability and complying with public records requests. District personnel shall monitor online activities of individuals who access the internet via a district-owned device.

Under certain circumstances, the Board may be required to disclose such electronic information to law enforcement or other third parties.

By using the district's network, internet access, email system, devices, or other technological resources, individuals consent to have this use monitored by authorized district personnel as described in this policy.

E. USE OF PERSONAL TECHNOLOGY ON SCHOOL SYSTEM PROPERTY

The use of any personal technology device is governed by all other applicable Board policies, the Student Code of Conduct, Employee Handbook, and any other restrictions established by the school or district administration. The District assumes no responsibility for personal technology devices brought to school.

F. SECURITY/CARE OF PROPERTY

Security on any computer system is a high priority, especially when the system involves many users. All users are responsible for reporting information regarding security violations to appropriate personnel. Unauthorized attempts to log onto any school system computer on the District's network as a system administrator may result in cancellation of user privileges and/or additional disciplinary action. Any user identified as a security risk or having a history of problems with other systems may be denied access.

Users of district technology resources are expected to respect district property and be responsible in using the equipment. Users will follow all instructions regarding maintenance or care of the equipment and must comply with the Modern Learning Device Handbook. Users will be held responsible for any loss or damage caused by intentional or negligent acts in caring for devices while under their control.

G. PERSONAL WEBSITES AND SOCIAL MEDIA

The district may use any means available to request the removal of personal websites that substantially disrupt the school environment or that utilize the school system or individual school names, logos, or trademarks without permission.

Students

Although school personnel generally do not monitor students' internet activity conducted on non-school system computers during non-school hours, when a student's online behavior has a direct and immediate effect on school safety or maintaining order and discipline in the schools, the student may be disciplined in accordance with Board policy.

Employees

All employees are required to use resources approved by Dorchester School District Two when creating or utilizing websites for any and all educational and work-related postings or communications with students. Thus, employees may not use unapproved personal websites, applications, or online networking profiles to post information in an attempt to communicate with students about school-related matters.

Employees are to maintain an appropriate relationship with students at all times. Having a public personal website or online social media profile or allowing access to a private website or private online social media profile is considered a form of direct communication with students. Employees are encouraged to block students from viewing any material or social media profiles that are not age appropriate. Any employee found to have created and/or posted inappropriate content on a website or social media profile that has a negative impact on the employee's ability to perform his or her job as it relates to working with students or colleagues will be subject to discipline, including dismissal. This section applies to all employees, volunteers and student teachers working for or in Dorchester School District Two.

Anyone who wishes to establish an external website for specific district offices, initiatives, schools, or programs must first contact the public information office.

H. DISCLAIMER

The Board makes no warranties of any kind, whether express or implied, for the service it is providing. The Board will not be responsible for any damages suffered by any user. Such damages include, but are not limited to, loss of data resulting from delays, non-deliveries or service interruptions, whether caused by the district’s or the user’s negligence, errors, or omissions. Use of any information obtained via the Internet is at the user’s own risk. The district specifically disclaims any responsibility for the

accuracy or quality of information obtained through its internet services.

Legal References: U.S. Const. amend. I; Children's Internet Protection Act, 47 U.S.C. 254(h)(5); Electronic Communications Privacy Act, 18 U.S.C. 2510-2522; Family Educational Rights and Privacy Act, 20 U.S.C. 1232g; 17 U.S.C. 101 *et seq.*; 20 U.S.C. 6777; G.S. 115C-
325(e) (applicable to career status teachers), -325.4 (applicable to non-career status teachers)