DORCHESTER SCHOOL DISTRICT TWO

STAFF DEVICE HANDBOOK

TABLE OF CONTENTS

OVERVIEW

Dorchester School District Two desires to be recognized as a "World Class" school district, providing all members of our district family with an environment that permits them to do their professional and personal best. All certified staff members will receive a device in order to support access to information, promote modern learning strategies and initiatives, enhance communication and collaboration, and innovatively create while safely, ethically, and successfully utilizing technology. This handbook outlines the expectations for device use, while providing staff members with procedures for appropriate use, care of, and security.

RECEIVING A DEVICE

A district-issued device will be distributed following each school's Staff Device Deployment and Orientation. All certified staff members will be issued a device for use at school, home, and through the summer as appropriate. In order to receive a district-issued device and gain access to the district network, all staff members are required to:

- Read, agree to, and follow the guidelines established in the following:
  - Dorchester School District Two Staff Device Handbook
  - Policy GBEEB – Technology Responsible Use
  - AR GBEBD-R – Use of Technology Resources in Instruction
- Electronically sign the District-Issued Device Acceptable Use Agreement (AUA) (Appendix A).
- Attend the device deployment orientation.

RETURNING A DEVICE

Staff members transferring out of or leaving Dorchester School District Two for any reason (moving, retirement, etc.) during the school year must return the district-issued device, including accessories, within 72 hours of the last day of employment to their current school Media Center or District Office Technology Center.

- The district-issued device and device accessories must be returned with only normal wear and no alterations. One power cord and one protective case will be provided to each certified staff member upon initial device reception. Cords and chargers should be maintained and returned in working order.
- If a staff member does not return his/her device and device accessories to the individual school/work site prior to leaving Dorchester School District Two, or at any time designated by school or district administration, it may result in the device being reported stolen and police involvement initiated to recover the device. The staff member may be subject to criminal prosecution or civil liability and may be required to pay the full replacement cost for a new district-issued device and accessories.

DEVICE IDENTIFICATION

- Each certified staff member's district-issued device will be labeled/barcoded in the manner specified by the district.
- Writings, drawings, stickers, and labels on the device are prohibited.

GENERAL CARE OF THE DEVICE

The district-issued device is the property of Dorchester School District Two. All users will follow these guidelines and the District-Issued Device Acceptable Use Agreement (AUA). Each certified staff member is individually responsible for the general care of his/her assigned device.

General Precautions

- Keep the device away from food, beverages, direct sunlight, extreme cold, sinks, water fountains, or any other area that may cause damage to the device.
- Devices should not be used or left in areas that may lead to damage or theft.
- Staff members are responsible for making sure files are backed up.

Transporting and Storing the Device

Devices are equipped with a protective case to aid in the prevention of accidental damage and should not be removed. The case is not entirely effective in preventing damage; staff members should take proper care of the device at all times.

Screen Care

Screen damage often occurs when pressure is applied to the screen.

- When in transition, the devices should be closed and secured.
- Before closing the device, staff members should ensure the keyboard is clear of all obstructions.
- If the device screen requires cleaning, only a clean, dry, cloth should be used. The use of cleansers of any type is prohibited.

STAFF RESPONSIBILITIES

- Devices should never be left unsecured; staff members are responsible for the security of their device at all times, both on and off district property.
- Staff members will be held responsible for all usage of and content stored on the device.
- Staff members are prohibited from loaning their device to another person, including family members.
- Staff members are prohibited from attempting to download applications, programs, disable or uninstall the virus protection program that is provided with the device, or view inappropriate content on individually issued student devices.
- District-issued devices are subject to routine monitoring by authorized staff. Users shall have no expectation of privacy while using the district-issued device.
- Staff members are responsible for maintaining the security of all usernames and passwords issued to them. Account usernames and passwords are never to be shared. This includes network, software, and web-based application usernames and passwords.
- Any modifications made in the device's settings will be for usability or visibility reasons only.

LOSS, THEFT, and DAMAGE

As with any piece of school property checked out to staff members, the staff member is responsible for their assigned district-issued device. Situations involving loss, theft, or damage of the device will be dealt with on a case-by-case basis.

Terms of the District-Issued Device Acceptable Use Agreement (AUA)

Terms and conditions that apply to the usage of the district-issued device are as follows:

- The district will cover parts and repairs for system-related issues or malfunctions of the device.
- The district will cover parts and repairs for ONE incident of accidental damage, such as cracked screens, liquid damage, or cosmetic damage.
- The district will not cover intentional damage or damage due to negligence or loss.
- The district will not cover theft without a documented police report that clearly shows forced entry into a secured location.
- The district will provide staff members a replacement device upon review of loss, theft, or damage.

Loss

- Devices left unattended in an unsecured location cannot be considered stolen; they will be treated as lost devices.
- A lost device is not covered by the district and must be reported immediately to the staff member's school/work site administrator/supervisor.
- The staff member may be responsible for compensating the school district.
- For a lost device, charging cable, protective case, and/or any other accessories for the full replacement value of the item if negligence is determined.
- A refund will be issued if the lost item is recovered and turned in to the school technology center by the end of the current school year. The refund will only be issued if the barcode is intact, the barcode matches the originally assigned staff member, and the item is still in working condition.

Theft

1. A stolen device must be reported immediately to law enforcement and a documented police report obtained by the staff member.
    a. A documented police report is required and must clearly indicate forced entry into a secured location. Obtaining the report and submitting it to the school/work site is the responsibility of the staff member.
    b. Failure to report a stolen device will result in the staff member being held financially responsible for replacement of the device.
2. The stolen device must also be reported to the staff member's school/work site administrator/supervisor and Media Specialist.
    a. The school Media Specialist will issue a replacement device.
3. Staff members should never attempt to recover a stolen device.

Damage

- Malfunctioning or damaged devices must be reported to technology support immediately.
- The district will not cover intentional damage or damage due to negligence or loss.
    - Decisions regarding neglect, intentional damage, and misuse will be made by school administration, district technology staff and/or the authorized repair representative.
- The district will be responsible for parts and repairs for ONE accidental damage, such as cracked screens, liquid damage, or cosmetic damage.
- Staff members should not attempt to repair or take the district-issued device to an outside repair source. Doing so will invalidate the warranty and the staff member will be responsible for the cost(s) associated with the damage. Staff members should take their district-issued device to the school/work site to have a district technology team member examine it.
- The staff member is responsible for compensating the school district for repairs or replacement costs due to intentional damage, negligence, misuse, and/or violating the District-Issued Device Acceptable Use Agreement (AUA).

User Misuse and Abuse Costs

If a district-issued device or accessories is misused or abused, the staff member is responsible for the cost of repair. Repair costs for a district-issued device or accessories due to deliberate damage or neglect may include, but are not limited to:

- Broken device screen
- Damaged device keyboard, device or docking station power cord, or protective device case
- Broken or damaged monitor, wireless keyboard or mouse, docking station, or active pen

Note: Repair costs shall not exceed the full replacement price of the device.

Repairs and Replacement

- Refer to **Appendix B** for information about district-issued device coverage.
- Refer to **Appendix C** for replacement and repair pricing.

USING THE DEVICE RESPONSIBLY

District Network Connectivity

For the best network experience, staff devices should be connected to the district network using a hardline connection. Staff devices may also be configured to connect to a district wireless network using individual staff login credentials and should remain on that designated network while on any district campus. The use of proxy servers or VPNs to bypass district network filters is prohibited.

International Connectivity

Due to network security, district-issued devices are unable to access the network outside of the United States and Canada.

Limitation of Liability

While Dorchester School District Two employs filtering, safety, and security mechanisms and attempts to ensure their proper function, it makes no guarantee as to its effectiveness.
Dorchester School District Two will not be responsible, financially or otherwise, for unauthorized transactions conducted using the device.

Home Internet Access

- Staff members may establish wireless connections with their device outside of school wherever access is available.
- District internet filters are applied outside of school and when using Dorchester School District Two internet connections. While this filtering solution is effective, the district cannot guarantee that access to all inappropriate sites will be blocked.
- Dorchester School District Two is not responsible for issues experienced or information obtained while on the home network or internet.
- Dorchester School District Two will not serve as the internet service provider for staff home use. For staff members to access the internet at home, the staff member must subscribe through an internet service provider. If staff members do not have home internet access, there are a variety of options for connecting to the internet including, but not limited to, public libraries and public businesses that provide free Wi-Fi access to patrons.

District Responsibilities for Digital Citizenship

- The district and school will comply with both federal and state laws regarding staff internet use, such as FERPA, CIPA, and COPPA.
- The district employs and maintains internet filtering, online monitoring of staff activity, and security mechanisms.
- Dorchester School District Two reserves the right to investigate any inappropriate use of resources and to review, monitor and restrict information stored on or transmitted via Dorchester School District Two district-owned equipment and resources.

TECHNOLOGY SUPPORT

- DDTwo eLearning webpage: https://www.ddtwo.org/tech
- Student MLS Support Form
- Staff MLS Support Form
- Technology Resources Notebook
- Cantey Tech Consulting:
    - help@canteytech.com
    - Staff Support: (843) 561-9700 or ext. 9700
    - Student Support: (843) 896-0777

FERPA

The Family Educational Rights and Privacy Act (FERPA) is a federal law that affords parents and students over 18 years of age certain rights with respect to students' educational records including photographs. Staff must obtain administrative permission to publish or make publicly available a photograph or video of any school-related activity. Unauthorized recordings are subject to disciplinary action in accordance with the district's Acceptable Use Agreement.

TITLE

Legal title to the property is with the district and shall, at all times, remain with the district. A staff member's right of possession and use is limited to and conditioned upon his/her full and complete compliance with the District-Issued Device Acceptable Use Agreement (AUA). The staff member is responsible for the care, use, and security of the device and accessories at all times.

REPOSSESSION

Dorchester School District Two reserves the right to repossess a device at any time if the staff member does not comply with all terms of the District-Issued Device AUA.

APPROPRIATION

Failure to return the property as requested by school administration will result in the staff member being referred to local law enforcement.

MODIFICATION TO PROGRAM

Dorchester School District Two reserves the right to modify this program or its terms at any time.

APPENDIX A: DISTRICT-ISSUED DEVICE ACCEPTABLE USE AGREEMENT

Technology Assigned to Classroom Workspace

I understand that the items listed below are issued to a physical space and are not to be removed by individuals. I agree to be held responsible for any of the items listed above if they are lost or damaged due to personal negligence.

As an employee of Dorchester School District Two, I understand and agree to be held responsible for the following technology issued to my classroom/workspace

- ☐ Dell 24-inch Monitor (P2419H) with Applicable Cords
- ☐ Dell Docking Station with Power Cord
- ☐ If Applicable: Cisco Telephone

Technology Assigned to Staff

I understand that the items listed above are assigned to me through the District's Asset Management System. I agree to be held responsible for any of the items listed above if they are lost or damaged due to personal negligence.

As an employee of Dorchester School District Two, I understand and agree to be held responsible for the following technology:

- ☐ Dell 5310 2-in-1 Business Laptop
- ☐ Optional: Dell Wireless Keyboard and Mouse
- ☐ Optional: Dell Premium Active Pen

As a borrower of a Dorchester School District Two device, I agree and accept the following responsibilities:

- ☐ I have read, agree to, and will follow the guidelines established in the following:
    a. Dorchester School District Two Staff Device Handbook
    b. Policy GBEEB – Technology Responsible Use
    c. AR GBEBD-R – Use of Technology Resources in Instruction

- ☐ I will use the device for work-related purposes and understand that the device is not to be loaned to anyone.

- ☐ I will not write on or place any labels or stickers on the district device. Any modifications I make in the device's settings will be for usability or visibility reasons only.

- ☐ I will not install software or hardware on a district device or network, or disable or uninstall the virus protection program that is provided with the device. I understand that software and hardware requests must be approved by the District Office and can only be installed by Cantey Tech Consulting.

- ☐ I will report any problems/issues I encounter while using the device to the technology department immediately through the help desk. (Cantey Tech Consulting – 843-561-9700).

- ☐ I understand that I am responsible for maintaining proper backups of locally stored data in order to minimize data loss should the district device become corrupt or rendered inoperable. I understand that reimaging the device may be a course of action for any repairs or modifications on the device, and this will result in the loss of all data stored on the laptop's hard drive.

- ☐ I understand that I am responsible for notifying my school principal or supervisor immediately in the event the device is stolen or lost, and that I must provide the school or district with a copy of a filed police report for stolen devices.

- ☐ I will follow the guidelines listed below for proper care and security of the device:

    - Keep food and drink away from the device.
    - Do not leave the device exposed to direct sunlight or extreme cold.
    - Do not attempt to repair a damaged or malfunctioning device.
    - Do not attempt to upgrade the device or software.

- ☐ Proper security is to be provided for the device and accessories at all times, including but not limited to the following:

    - Secure the device and any device accessories when not in use.
    - Unattended devices should be left on a "lock screen" to protect privacy.
    - Do not leave the device or accessories in an unlocked car.

- ☐ I understand that all devices, equipment, and/or accessories that the district has provided to me are the property of Dorchester School District Two. Additionally, I understand that I will not be held responsible for device, equipment, or accessory issues resulting from regular school-related use; however, I understand that I am responsible for any damage, theft, or loss of the device and/or related equipment or accessories due to negligence. I understand that a violation of the terms and conditions set out in the District-Issued Device Acceptable Use Agreement (AUA) will result in the restriction and/or termination of my use of the district's devices, equipment, and/or accessories, and may result in further disciplinary actions including termination of employment and/or legal action.

Signature: _____

Date: _____

APPENDIX B: DISTRICT-ISSUED TECHNOLOGY COVERAGE

The district will cover costs associated with the following:

- First repair of device due to accidental damage (as determined by the authorized repair representative), and/or
- Replacement of a stolen device (unless stolen due to staff negligence)
    - Staff must submit a police report within 48 hours in order to be issued a replacement device (limit of one replacement).

The district will not cover costs associated with the following:

- Repairs due to accidental damage in excess of one occurrence,
- Repairs due to intentional damage, neglect or misuse of the device,
- Repairs of damage caused by violating the Acceptable Use Agreement (AUA),
- Repairs due to a staff member attempting to repair, reconfigure or reset the device (any attempt to tamper with the internal components of the device will be considered intentional damage),
- Replacement of a stolen device due to staff negligence,
- Replacement of more than one stolen device not due to negligence (limit of one replacement),
- Replacement of a lost device and/or accessories.

APPENDIX C: REPLACEMENT/REPAIR PRICING

District-Issued Device and Accessories Replacement Pricing

Item	Price
Dell 5310 2-in-1 Business Laptop Replacement	$795
Dell Screen Replacement (including webcam built in)	TBD
Dell EE System Board Replacement	TBD
Dell Top Cover with Keyboard Replacement	TBD
Dell Webcam in Top Cover Replacement	TBD
Dell Charging Cord Replacement	$20
Dell Wireless Keyboard and Mouse Replacement	$15
Dell Premium Active Pen Replacement	$45
Dell 24-inch Monitor (P2419H) Replacement	$100
Dell Docking Station Replacement	$84
Gumdrop Cover for Dell 5310 Replacement	$16

APPENDIX D: POLICY GBEEB – 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 Student 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, Student 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, timekeeping 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 Student 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.

For security purposes, Cantey Tech Consulting/Dorchester Two does not allow for the installation of print drivers or Wi-Fi printer access on a student device for use with printing to a personal home printer. In the event students want to print a file, files may be uploaded to the student MS OneDrive account and accessed from a computer with printing capabilities.

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 Student 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)

APPENDIX E: AR GBEBD-R – USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

Introduction

In making decisions regarding access to technology, Dorchester School District Two considered its educational mission, goals and objectives. Electronic access to information and the research and analysis skills required for its effective use are now fundamental to the preparation of citizens and future employees. Access to network computer technologies enables students to explore libraries, databases, websites and other resources while communicating with people around the world.

The district expects that faculty will blend the use of these technologies throughout the curriculum and will provide guidance and instruction to students in its proper and responsible use. As much as possible, access to Internet resources should be structured in ways which point students to acceptable uses of those resources. While students will often be able to move beyond staff approved resources, guidelines and lists of resources particularly suited to learning objectives will be provided to them.

Outside of school, families bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies and other possibly offensive media.

General access to technology

Dorchester School District Two provides its employees and students with access to computing equipment, systems and network functions such as e-mail and the Internet. This access has a limited educational purpose for students and is to facilitate employees' work productivity. Students and employees utilizing and/or observing school-provided Internet access are responsible for good behavior online just as they are in a classroom or other area of the school. The same rules for behavior and communications apply.

Education, supervision and monitoring

It is the responsibility of all members of Dorchester School District Two to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this AUP policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act and the Protecting Children in the 21st Century Act.

Procedures for disabling or otherwise modifying any technology protection measures will be the responsibility of the technology department or designated representatives.

Students and staff must be instructed on the appropriate use of the network, Internet and e-mail services.

<u>Employees</u>
All district employees are required to complete initial network computing orientation and training. Dorchester Two also offers extensive professional development opportunities in the use of supported computing tools and technology, Internet safety, cyberbullying prevention and social media guidelines. Employees are

expected to retain proficiency in computing resources as required by their professional capacity as public educators.

Students

Prior to technology use, all students will receive basic orientation and training on the responsible use of technology. Orientation may include, but is not limited to, Internet safety, responsible social media use and cyberbullying. District personnel or designated representatives will provide age-appropriate training for students using computing and network services. The training provided will be designed to promote Dorchester Two's commitment to the following.

- the standards and acceptable use of Internet services as set forth in this acceptable use policy student safety with regard to the following
- safety on the Internet
- appropriate behavior while on online, on social networking Web sites and in chat rooms
- cyberbullying awareness and response
- full compliance with the requirements of the Children's Internet Protection Act (CIPA)

Following receipt of this training, students will acknowledge that they received the training, understood it and will follow the provisions of the district's acceptable use policies.

All students and staff must sign a form acknowledging that they have read and understand the acceptable use of technology policy and administrative rules; that they will comply with the policy and administrative rules; and that they understand the consequences of violating the policy or administrative rules.

Filtering and Security

The district deploys targeted technologies within its computer networks designed to filter and secure them from outside intrusion and inappropriate materials. These measures include active web-filtering technologies as required by the Child Internet Protection Act, email spam filtering and other network monitoring devices as needed.

Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Users are prohibited from tampering or otherwise attempting to circumvent filtering technologies through any means and should report any observed attempt to do so through third-party "proxy" servers, shared network credentials or other forms of "hacking".

Should a user find an educationally appropriate resource blocked by a filter, they may request that it be allowed by contacting the school-based instructional technology specialist.

Personal privacy

Communications conducted over district networks, including voicemail messages, email, attached documents and images are not private. All records generated within the district (except those specifically excluded by law), whether in electronic or hardcopy form, are subject to the Freedom of Information Act and open to public inspection.

Dorchester School District Two reserves the right for system administrators to examine, restrict or remove any material that is on or passes through its technology systems.

Users are asked to use good judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.
Users may not reveal home addresses, personal e-mail addresses or personal phone numbers of colleagues or students as it is a violation of district policy.

Use of system resources

System resources are limited and are intended to support the educational objectives of Dorchester School District Two.

The use of technology systems must be consistent with and support educational objectives. Therefore, activity on the network, such as Internet sites accessed, communications via email, listservs, forums, chat rooms, web applications or forms of social media must support the district's objectives.

Network file storage is limited, and users should regularly review and delete unnecessary files, email messages, voicemail messages and other network-hosted content.

Users should make a conscientious effort to conserve district resources. Use of high bandwidth resources, such as videoconferencing, online music or streaming video must be related to educational goals and authorized by the technology department.

Users are responsible for backing-up copies of documents and data that are important to their jobs or assigned tasks. The district is not responsible for the loss of personal data.
Using email to send chain letters, advertisements, personal notices or engaging in "spamming" (sending an annoying or unnecessary message to large numbers of people) is in violation of this policy.

Outside use of district technology

Many network resources provided by the district are connected to the broader Internet and accessible from outside its school and office locations. Employees and students using these services should use the same discretion and adherence to district policy while accessing those platforms as they would from work or school. District-owned devices and peripherals used from home to access Internet resources on private Internet wireless or cellular networks are also subject to this policy and should not be used for proscribed activities or to view inappropriate material.

Personal websites and Internet use

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.

<u>Students</u>
Although school personnel generally do not monitor students' Internet activity conducted on non-school system computers during non-school hours, when a student's on-line 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 or on-line 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 on-line social media profile or allowing access to a private website or private on-line 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 school district offices, initiatives, schools or programs must first contact the public information office.

Student use of personal technology services

Dorchester School District Two does not generally support student use of personally owned technology devices on its network. Students may bring personal technology devices, including iPods, tablets/iPads, netbooks, laptops, music player devices, gaming systems and smart phones into a school with the permission of the building principal and must utilize personal technology devices in compliance with all district and school rules established as guidelines for their use.

Social media use by employees

Employees engaging in social media platforms (examples include Facebook, Twitter, LinkedIn, Instagram, etc.) for personal use should pay special attention to how information posted under the account could be viewed and disseminated publicly. Social media are powerful communication tools that must be used appropriately just like telephones, email, text messages and handwritten forms of communication. Some guidelines for successfully using social media are listed below.

Do

- Refrain from accepting current school district students as "friends" on personal social networking sites. Be aware that people classified as "friends" often have the ability to download and share your information with others.
- Remember that once something is posted to a social networking site, it may remain available online even if you think it is removed, and it may be far-reaching.

- Understand social networking privacy settings for each platform and set them at appropriately restrictive levels. Report, as required by law, any information found on a social networking site that falls under the mandatory reporting guidelines.
- Consider whether a particular posting puts your professional reputation and effectiveness as a district employee at risk.

Do not

- Use a social networking site to discuss students or employees.
- Use an unapproved social media platform to conduct school-related communication with parents or students.
- Post images or communications that include personal or revealing information about students or employees.
- Identify yourself as a representative of or spokesperson for the district, unless you have been approved to do so by the superintendent or the public information office. This includes using school logos, mascots, photographs or other such graphic representations or images associated with the district.

Anyone who wishes to establish a social media account for specific school district offices, initiatives, schools or programs must first contact the public information office. Social media may be used for school-related purposes only with the approval of the public information office. If you have questions, would like to start a social media initiative on behalf of a district entity or have content you would like posted to the district's online presence, please contact the public information office.

Cyberbullying

The use of networked technology for harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding and cyberstalking are all examples of cyberbullying. Sending emails or posting comments with the intent of scaring, hurting or intimidating someone else constitutes bullying. In some cases, cyberbullying can be a crime. These forms of activity should be reported immediately to the appropriate school authority.

Examples of acceptable use

I will do the following.

- Use school technologies for school-related activities and research.
- Follow the same guidelines for respectful, responsible behavior online that I am expected to follow offline.
- Treat school resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher, staff member, or administrator if I see threatening/bullying, inappropriate or harmful content (images, messages, posts) online.
- Use school technologies at appropriate times, in approved places for educational pursuits only.
- Cite sources when using online sites and resources for research to ensure there is no copyright infringement. Recognize that use of school technologies is a privilege and treat it as such.
- Be cautious to protect the safety of myself and others. Help to protect the security of school resources.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Examples of unacceptable use

I will not do the following.

- Use school technologies in a way that could be personally or physically harmful to me or others.
- Search for or view inappropriate images or content.
- Engage in cyberbullying, harassment or disrespectful conduct toward others-staff or students.
- Try to find ways to circumvent the school's safety measures and filtering tools.
- Use school technologies to send spam or chain mail.
- Plagiarize content I find online.
- Post personally-identifying information about myself or others.
- Impersonate another person or utilize technology resources to create false identities.
- Agree to meet someone I meet online in real life without a trusted adult present.
- Use language online that would be unacceptable in the classroom.
- Use school technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, accounts or content that isn't intended for my use.
- Access another individual's materials, information or files without their direct permission.
- Vandalize, damage, or disable the property of another individual or organization.
- Violate any local, state, or federal statute.

This is not intended to be an exhaustive list. Users should use their own good judgment when using school technologies.

Copyright

No employee or student of Dorchester District Two should engage in unauthorized copying, the use of copyright-protected material or violate the intellectual property rights of others. Teachers and employees unsure of copyright or "fair use" status of any material should seek further assistance from a qualified media specialist, administrator or instructional technology specialist before copying and/or distributing such content.

Disciplinary action

<u>Students</u>
Any violation of district policy and rules may result in loss of district-provided access to the Internet. Additional disciplinary action may be determined at the building level in keeping with existing procedures and practices regarding inappropriate language or behavior. When and where applicable, law enforcement agencies may be involved.

<u>Employees</u>
Employees in violation of this policy will be disciplined in accordance with established district policy up to and including termination of employment.

Indemnity

Dorchester School District Two makes no warranties of any kind, neither expressed nor implied, for the Internet access it is providing. The district will not be responsible for any damages users suffer, including, but not limited to, loss of data resulting from delays or interruptions in service. The district will not be responsible for the accuracy, nature, or quality of information stored on district storage media, hard drives or servers; nor for the accuracy, nature or quality of information gathered through district provided Internet access. The district will not be responsible for personal property used to access district computers or networks or for district-provided Internet access. The district will not be responsible for unauthorized financial obligations resulting from district-provided access to the Internet.

Evaluation and revision

This policy will be reviewed and updated annually on or by June 31st by the technology roundtable working group to reflect the changing nature of technology and its use in Dorchester School District Two.

Compliance

This policy and all its provisions are subordinate to local, state and federal statutes.

Appendix A: *CIPA definitions of terms:

Minor. The term "minor" means any individual who has not attained the age of 17 years.

Technology protection measure. The term ``technology protection measure'' means a specific technology that blocks or filters Internet access to visual depictions that are any of the following.

- obscene, as that term is defined in Title 18 of the United States Code Annotated, Section 1460 child pornography, as that term is defined in Title 18 of the United States Code Annotated, Section 2256 harmful to minors

Harmful to minors. The term ``harmful to minors'' means any picture, image, graphic image file or other visual depiction that is any of the following.

- taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex or excretion depicts, describes or represents in a patently offensive way, with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals
- taken as a whole, lacks serious literary, artistic, political or scientific value as to minors

Sexual act/contact. The terms ``sexual act'' and ``sexual contact'' have the meanings given such terms in Title 18 of the United States Code Annotated, Section 2246.

Issued 10/03; Revised 6/9