

DD2 Acceptable Use Policy

USE OF TECHNOLOGY RESOURCES IN INSTRUCTION

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.

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.

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 on page 89 of this handbook 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”.

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 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.

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.

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.

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.

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 INCLUDING BUT NOT LIMITED TO

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.

EXAMPLES OF UNACCEPTABLE USE INCLUDING BUT NOT LIMITED TO

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.

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

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.

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.

(Reference: AR GBEED-R Use of Technology Resources in Instruction. For the full administrative rule, visit do.ddtwo.org.)