Appropriate Use Policy

Jefferson Davis County School District

APPROVED
JUL 2 1 2022
BY SCHOOL BOARD

Scope

This Policy applies to all Users district technology, including but not limited to students, faculty, and staff. It applies to the use of all district technology. These include systems, networks, and facilities administered by the JDCS Office of Information Technology, as well as those administered by individual schools and departments.

Use of district technology resources, even when carried out on a privately owned computer that is not managed or maintained by Jefferson Davis County Schools, is governed by this Policy.

Policy

It is the policy of the Jefferson Davis County Schools to

1. Prevent the transmission of inappropriate material via the Internet.
2. Prevent unauthorized access to materials and unlawful online activities.
3. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors.
4. To comply fully with the Children's Internet Protection Act.

Purpose

The Jefferson Davis County School District (JDCS) is pleased to offer its student's access to the Internet. The Internet is an electronic highway connecting hundreds of thousands of computers and millions of individual users globally. This computer technology will help propel our schools through the communication age by allowing students and staff to access and use resources from distant computers, communicate and collaborate with other individuals and groups, and significantly expand their available information base.

Internet access is coordinated through a complex association of government agencies, and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the users who must adhere to strict guidelines. These guidelines are provided here so that you are aware of the responsibilities you are about to assume. In general, this requires efficient, ethical, and legal utilization of the network resources. If a JDCS District user violates any of these provisions, his or her account will be terminated and future access could possibly be denied.

The signature(s) at the end of this document is (are) legally binding and indicates the party (parties) who signed has (have) read the terms and conditions carefully and understand(s) their significance.

CIPA Definition of Terms:

Technology Protection Measure. The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are:

1. Obscene, as that term is defined in section 1460 of title 18, United States Code;

2. Child Pornography, as that term is defined in section 2256 of title 18, United States Code; or

3. Harmful to minors.

Harmful to Minors. - The term "harmful to minors" means any picture, image, graphic image file, or other visual depiction that:

1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

2. 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; and

3. Taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Sexual Act; Sexual Contact. - The terms "sexual act" and "sexual contact" have the meanings given such terms in section 2246 of title 18, United States Code.

1. A qualifying "technology protection measure," as that term is defined in Section 1703(b)(1) of the Children's Internet Protection Act of 2000; and

2. Procedures or guidelines developed by the superintendent, administrators and/or other appropriate personnel which provide for monitoring the online activities of users and the use of the chosen technology protection measure to protect against access through such computers to visual depictions that are (i) obscene, (ii) child pornography, or (iii) harmful to minors, as those terms are defined in Section 1703(b)(1) and (2) of the Children's Internet Protection Act of 2000. Such procedures or guidelines shall be designed to:

a. Provide for monitoring the online activities of users to prevent, to the extent practicable, access by minors to inappropriate matter on the Internet and the

World Wide Web;

b. Promote the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;

c. Prevent unauthorized access, including so-called "hacking," and other unauthorized activities by minors online;

d. Prevent the unauthorized disclosure, use and dissemination of personal identification information regarding minors; and

e. Restrict minors' access to materials "harmful to minors," as that term is defined in Section 1703(b)(2) of the Children's Internet Protection Act of 2000.

Internet Terms and Conditions of Use

1. Users will demonstrate legal responsibility by not transmitting any material in violation of United States, Mississippi, or Jefferson Davis County School District laws or regulations. This includes, but is not limited to: copyrighted materials, threatening, harassing, or obscene material, pornographic material, or material protected by trade secret.
2. Users have the responsibility to use computer resources for academic purposes only unless supervised by school staff.
3. Users may not conduct commercial activities for profit, advertise products, or conduct political lobbying on the network.
4. Users will not use the network for any illegal activity.
5. Users will not cause damage to any school equipment including hardware and software.
6. Users will not remove, exchange, or tamper with any hardware or software component from any system.
7. Users will not delete, rename, move, copy, or change any file or its properties, other than his/her personally owned files.
8. Users will not tamper with installed software and files.
9. Users will not attempt to gain access to unauthorized files.
10. Users will not attempt to change passwords.
11. Users will not damage other students' work.
12. Users will not install personal software on JDCS District Technology.
13. Users will not violate copyright laws by unauthorized copying of software.
14. Users will be responsible for citing sources and giving credit to authors during the research process. All communications and information accessible via the network should be assumed to be private property.
15. Users will not install, copy, or knowingly infect a computer system with a virus. 3
16. Users will not use email accounts for SPAM or chain letters.
17. Users will not use language that may be considered offensive, defamatory, or abusive.
18. Users will not attempt to defeat any security system.

Security

1. Users will not access the network using another user's account. 2. Users should consider their login and password private and should not reveal this information.
3. Users will not divulge information, personal or otherwise, about themselves or other users.
4. Users will immediately report to JDCS District authorities any attempt by other Internet users to engage in inappropriate conversations or personal contact.
5. Users should not expect that files stored on school-based computers will remain private. Authorized staff will periodically inspect personal folders and logs of network usage will be kept at all times.
6. Users are not allowed access to the computer operations area, and access is restricted to those responsible for operation and maintenance. No individuals are allowed in JDCS server or equipment rooms unless they are under close and immediate supervision of an IT staff member or authorized staff member. Tampering with equipment is prohibited.
7. Users consent to the use of scanning programs for security purposes by bringing any personal computers or technology onto school grounds.
8. Users consent to having user actions logged in order to facilitate recovery from system malfunction and for other management purposes.

Individual schools may create additional guidelines and procedures consistent with this policy. Such guidelines and procedures will be appropriate for the electronic information resources being used and the student served at the school. There will be consequences for any user who fails to follow JDCS District and school guidelines and policies. The consequences may include paying for damages, denial of access to technology, detention, suspension, or expulsion. In severe cases, the JDCS District will involve law enforcement authorities.

Private computers must not be used to provide network access. Students, Teachers, and Staff should not connect private computers to the JDCS Network without prior written permission from the JDCS District Director of Technology. Private computers must not use the JDCS network for commercial gain or profit. Students, Teachers, and Staff should not install or otherwise connect personal computer equipment to any computer, server, or network connection without prior written approval from the JDCS Director of Technology.

Users may not alter the JDCS network infrastructure by installing any unauthorized networking equipment including (but not limited to) hubs, switches, routers, or wireless access points of any kind without the express permission of the JDCS Information Technology Department. It is also a violation to install any

devices or programs on the JDCS network or any other PC or computing device connected to the JDCS network that are designed to alter, reshape, affect, monitor, or intercept network traffic.

The JDCS Information Technology Department may terminate or limit the network connectivity of any user whose online activities are deemed detrimental to the health of the network.

1. Software Copyright Laws

The Jefferson Davis county School District has made technology available to all staff and students. Computers, computer networks, the Internet, and computer software have been made available for the purpose of enhancing education in the classroom. The JDCS District is also committed to adhering to all copyright laws. All employees and students of the JDCS District are to abide by copyright laws as specified by the software's publishers and distributors.

The following rules have been put in place to ensure that no employee or student of the JDCS District violates any federal, state, or local regulation of copyright laws.

a. No software will be installed on any District computer without the proper license.
b. The only individual that signs software license agreements for the JDCS District is the Director of Technology.
c. Each department and/or school will establish a central location to store software licenses to be reviewed on demand.
d. Permission must be obtained from the JDCS District Director of Technology to duplicate any software product or distribution media.
e. Employees must receive permission from their principal and the JDCS District Director of Technology before purchasing software for District use.
f. Principals shall be responsible for enforcement of this policy at their individual school.

2. Violations

Employees who violate the United States Copyright Laws do so at their own risk and assume all liability for their actions. They shall also be subject to disciplinary action for willful infringement of the law or for using District equipment for duplication that is prohibited.

Purchasing Policy for Technology Equipment

It is the goal of the Office of Information Technology to assure that all computer hardware, peripherals, and software can be supported. The staff' members in the Office of Information Technology have the primary responsibility for maintaining the networks, computers, servers, printers, peripherals, and VoIP phones to be certain that quality is maintained at reasonable costs.

All equipment, computers and peripheral devices (e.g. printers, scanners, LCD projectors, digital cameras, software, video cards, network cards) which are attached to or used with a computer must be ordered only after consultation with the District Director of Technology. The review procedure for purchasing any technology equipment and software is intended to provide:

- a centralized point of information about technology items
- a district-wide inventory of hardware and software
- pricing advantages
- license compliance for software purchases
- hardware and software that can be supported

In order to coordinate and standardize on technology equipment and software purchases in a uniform and planned way so as to avoid duplicate selection which could make the maintenance and operations of the technology program difficult and costly, the following purchase procedure is to be used:

- Requisition submitted to the immediate Supervisor for review
- Requisition signed and approved by the District Director of Technology
- Purchase order approved and signed by the Business Manager and the item ordered, if within district/school budget constraints

The JDCS Information Technology Department will not support any technology related equipment that was not purchased in accordance with these guidelines. Support and service is limited to approved technology purchases of JDCS owned hardware and software. Legacy equipment may not be supported if the District Director of Technology has determined that the software/hardware has reached "end of life". Reasonable requests for support of "end of life" equipment can be made, and faculty may choose to accept responsibility for the upkeep of legacy hardware/software. This arrangement may be overridden if the JDCS District Director of Technology decides that the upkeep of "end of life" equipment is a financial burden on the JDCS District. JDCS Information Technology staff may not provide support or services of equipment not purchased and owned by the JDCS District.

Guest Account Agreement

I understand and will abide by the above Appropriate Use Policy. Further, I understand that any violation of the regulations above is unethical and may constitute a criminal offense.

I hereby release the Jefferson Davis County School District from all claims and damages arising from my use of the JDCS Network.

This account has been created for the purpose of_____
I understand this account will be deleted within 15 days of work completion. I understand that it is my responsibility to remove all personal files and I will not hold the Jefferson Davis County School District responsible for any loss of data.

Name:_____

Position:_____

School/Department: _____

Signature: _____

Date: _____

Employee Account Agreement

I understand and will abide by the above Appropriate Use Policy. Further, I understand that any violation of the regulations above is unethical and may constitute a criminal offense. I understand that violation of the rules may result in disciplinary action up to and including termination of employment.

I hereby release the Jefferson Davis County School District from all claims and damages arising from my use of the JDCS Network.

Name:_____

Position:_____

School/Department: _____

Signature: _____

Date: _____

Student Account Agreement

Student

I have read the information written above. If I did not understand the meaning of a part of it, I asked an adult to explain it to me. I understand and will abide by the above Appropriate Use Policy. Further, I understand that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation, my Internet access privileges may be revoked, school disciplinary action may be taken, and/or appropriate legal action.

I hereby release the Jefferson Davis County School District from all claims and damages arising from my use of the JDCS Network.

Student Name:_____

Home Room:_____

School:_____

Student Signature:_____

Date:_____

Parent or Guardian

As the parent or guardian of this student, I have read the Appropriate Use Policy. I understand that this access is designed for educational purposes. The Jefferson Davis County School District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to restrict access to all controversial materials and I will not hold them responsible for materials acquired on the network. I have spoken with my child to make sure that the rules are understood. Further, I accept full responsibility for supervision if and when my child's use is not in a school setting. I hereby give permission to issue an account for my child and certify that the information contained on this form is correct.

My son or daughter, who has signed above, understands the rules that he or she is to follow in utilizing technology at school.

Parent or Guardian (please print):_____ Date:_____

Parent or Guardian Signature:_____