Technology Acceptable Use Policy
EMPLOYEE Acknowledgement Form
(updated August, 2019)

Dallas School District (DSD) Policy No. 815 USE OF THE INTERNET AND DISTRICT'S NETWORK (815) and all DSD Policies govern the use of technology in accordance with the language within 815.

All DSD technology users (users) are required to review 815 and to seek clarification from their immediate supervisor and to complete this binding acknowledgment form annually and upon accepting employment.

The purpose of this form is to highlight sections of 815; however, 815 should be reviewed and adhered to in its entirety and can be found at:

https://go.boarddocs.com/pa/dall/Board.nsf/Public?open&id=policies

Employees of DSD are reminded that all DSD policies apply to the use of technology, including but not limited to Policy No. 317 EMPLOYEE CONDUCT DISCIPLINE (317.) Policy No. #815 should be considered in the context of Policy No. 317 related to administrative directives and the progressive discipline model set forth within.

Highlights from Policy No. 815

Authority

The District is committed to ensuring internet safety to the greatest extent possible. This Policy governs the appropriate use of the District's network, District-owned technology and the internet, as set forth below. The provisions of this policy apply to all use of the District's network, both on and off campus as well as student and employee access to/use of the internet during school hours, on school grounds and during school-sponsored activities.

The Board shall provide access to computers, network, Internet, electronic communications, information systems, databases, files, software, and media (collectively called CIS systems), if there is a specific school district-related purpose to access information; to research; to collaborate; to facilitate learning and teaching; and to foster the educational mission, vision and beliefs of the school district.

Access to the School District's network is a privilege, not a right. The school district reserves the right to deny access to prevent unauthorized, inappropriate or illegal activity, and may revoke

those privileges and/or administer appropriate disciplinary action. The school district will cooperate to the extent legally required with ISP, local, state and federal officials in any investigation concerning or related to the misuse of the District's network. 47 U.S.C. § 254(l); 24 P.S. § 510; 24 P.S. § 4604.

Users have no privacy expectations in the contents of their personal files, or any of their use of district's network. The district reserves the right to monitor, track and/or log user access, as well as monitor and allocate file server space and access all user files. Users of the district's CIS systems who transmit or receive communications and information shall be deemed to have consented to having the content of any such communications recorded, checked, received, monitored, tracked, logged, accessed and otherwise inspected or used by the school district and to the district's monitoring and allocating file server space.

The school district has the right, but not the duty, to inspect, review or retain electronic communication created, sent, displayed, received or stored on or over its CIS systems; to monitor, record, check, track, log, access or otherwise inspect; and/or report all aspects of its CIS systems use.

The school district reserves the right to:

1. Discontinue network availability and/or access at any time for any or all users for any reason;

2. Determine which network services and/or District technology will be provided through school district resources;

3. Determine the types of files that may be stored on school district file servers and computer;

4. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the District's network and electronic communications systems and/or on District technology, including email, text messages, and other electronic communications;

5. Remove from the network, District servers or District-owned devices, excess email and other electronic communications or files for any reason;

6. Revoke user privileges, remove user accounts, or refer to legal authorities, and or school district authorities when violation of this and any other applicable school district policies, regulations, rules, and procedures occur or ISP terms, or local, state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, vendor access, and destruction of School district resources and equipment.

Guidelines

CIS systems accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. CIS users shall respect the privacy of other users on the system.

Parental Notification and Responsibility

The school district shall notify the parents/guardians about the school district's CIS systems and the policies governing their use. This policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the school district to monitor and enforce a wide range of social values in student use of the Internet. Further, the school district recognizes that parents/guardians bear primary responsibility for transmitting their particular set of family values to their children. The school district shall encourage parents/guardians to specify to their children what material is and is not acceptable for their children to access through the school district's CIS system. Parents/Guardians are responsible for monitoring their children's use of the school district's CIS systems when they are accessing the systems beyond the school campus.

School District Limitation of Liability

The school district makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the school district's CIS systems will be error-free or without defect. The school district does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the school district; nor is the school district responsible for the accuracy or quality of the information obtained through or stored on the CIS systems. The school district will not be responsible for any damage users may suffer, including, but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the CIS systems. The school district will not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The school district shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the school district's CIS systems. In no event will the school district be liable to the user for any damages, whether direct, indirect, special or consequential, arising out of the use of the CIS systems.

Prohibitions

Students and staff are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Illegal activity.
2. Commercial or for-profit purposes.
3. Product advertisement or political lobbying.
4. Bullying/Cyberbullying or other type of harassment prohibited by law, the Student Code of Conduct or Board policy.
5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.[4]
8. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors.
9. Use of inappropriate language or profanity.
10. Transmitting material likely to be offensive or objectionable to recipients.
11. Intentionally obtaining or modifying files, passwords, and data belonging to other users.
12. Impersonation of another user, anonymity, and pseudonyms.
13. Fraudulent copying, communications, or modification of materials in violation of copyright laws.[15]
14. Loading or the use of unauthorized games, programs, files, or other electronic media. All programs, games, files, and electronic media must have approval of the Director of Technology prior to loading or usage.
15. Disrupting the work of other users.
16. Destroying, modifying, or abusing network hardware and software.
17. Quoting, summarization or other recounting of personal communications in a public forum without the original author's prior consent.
18. Communication of private/personal information of others.
19. Participation in online auctions or online gaming and/or gambling.
20. Use of the school's name, logos and web materials in personal communications.

21. Any suggestion that the employee or student represents the school in online activities.

22. Employee/Student communications considered to be boundary invasions.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, these guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.

2. Users are not to use a computer that has been logged in under another student's or employee's name.

3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Safety

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher, administrator, or Director of Technology.

Network users shall not reveal personal information to other users on the network, email, Internet, etc.

Internet safety measures shall effectively address the following:

1. Control of access by minors to inappropriate matter on the Internet.
2. Safety and security of minors when using electronic mail and other forms of direct electronic communications.
3. Prevention of unauthorized online access by minors, including "hacking" and other unlawful activities.
4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.
5. Restriction of minors' access to materials harmful to them.

_____ _____

EMPLOYEE LAST NAME - PRINT ALL CAPS **BUILDING - PRINT ALL CAPS**

DALLAS SCHOOL DISTRICT

2019

EMPLOYEE TECHNOLOGY ACCEPTABLE USE POLICY ACKNOWLEDGEMENT FORM

I understand and will abide by Policy No. 815, all DSD policies, and all protocols and conditions for technology usage. I further understand that any violation of the above regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, employee disciplinary action and/or appropriate legal action may be taken.

Employee Signature_____ Date_____

Employee Full Name (please print)_____

Building_____Grade_____Department_____