

Policy IJNDB Use Of Technology Resources

Issued 2/14

Purpose: To establish the board's vision and the basic structure and procedures for the use of technology resources.

Objective

This policy governs the use of technology resources in School District Five of Lexington and Richland Counties (District Five). It will allow the district to acquire the benefits of increased efficiency through the use of technology while protecting the district's information assets, the instructional and operational integrity of the district and the rights of students and district employees.

Definition

For the purposes of this policy, "technology resources" is defined as any technology equipment and/or resources used in the instructional, operational and/or administrative functions of the district. This includes, but is not limited to, computers, mobile devices, printers, scanners, servers, cabling, network electronics, email, and software.

Ramifications for Inappropriate Use

Inappropriate use of district technology resources will not be tolerated. Employees who fail to fully comply with this policy will be subject to administrative and disciplinary action(s).

The student disciplinary code will determine the actions taken against any student who does not fully comply with this policy.

Internet Access and Usage

District Five provides in-school Internet access for all students, teachers, and staff. The intent of this access is to facilitate teaching and learning. When used properly, use of the Internet promotes communication between all members in the learning community and has a positive impact on teaching and learning. Through Internet access, students, parents/legal guardians, and educators will have increased access to learning resources and opportunities. These opportunities will extend to the home, other educational institutions, and libraries or at any other location at which the Internet can be accessed.

District Five will take prudent actions to limit access to inappropriate websites and other information. However, due to the vast nature of the Internet, it is impossible to control all of the available information that is accessible; information appears, disappears, and changes constantly. It is not possible to predict or completely control what students and employees may locate via the Internet.

While reasonable steps will be taken, District Five cannot ensure the integrity of the Internet information accessed via the district's network resources. The school district makes no guarantees as to the accuracy of information received on the Internet. Although students will be under teacher supervision while on the Internet, it is not possible to constantly monitor every individual student and what they are accessing on the Internet. Some students might encounter information that is not of educational value.

Measures of Protection in Accessing Inappropriate Sites

Internet activities will be monitored by the district to ensure students and staff members are not accessing inappropriate sites. This includes websites that have visual depictions that contain obscenity, pornography, child pornography, and/or images that are otherwise harmful to minors or that incite violence. The school district will use technology protection measures (such as Internet filtering) to protect students from inappropriate access.

The district will provide reasonable notice of and at least one public hearing or meeting to address and communicate its Internet safety measures on an annual basis.

Reporting Child Pornography

District technology staff and school computer technicians who are working with a computer and discover sexually explicit images of children must report this to local law enforcement and appropriate district personnel. The report must include the name and address of the owner or person in possession of the computer. Failure of any district employee to properly notify law enforcement of discovered pornography on district technology will result in administrative and disciplinary action(s).

Acceptable Use Guidelines

District Five provides technology resources for use by students, teachers, and staff. The intent of these resources is to provide tools that will help facilitate teaching and learning. As such, students, teachers, and staff must adhere to the following guidelines when using technology resources.

Examples of acceptable use of District Five technology resources include, but are not limited to, the following.

- use of resources for educational purposes only
- use of resources in compliance with all local, state, and federal laws including, but not limited to, laws that govern copyright and intellectual property
- use of resources responsibly and with respect for others
- safeguarded accounts, passwords, and private information of staff and students
- installation and use of only software that has been legally obtained, licensed, and authorized for use on district technology resources

The following are improper uses of technology resources and are prohibited in District Five.

- transmitting any material which is in violation of any federal or state regulation (this includes, but is not limited to, copyrighted materials, threatening, or obscene material or material copyrighted by trade secret)
- using a computer to create, use, or download materials which would not be permissible in District Five classrooms in any other form (e.g., obscene, profane or pornographic materials)
- unauthorized access to or duplication of computer programs, systems, or data files
- unauthorized storage and/or loading of a computer program, system, or data file
- deliberate deletion/destruction of any computer programs, systems, or data files
- providing system access to unauthorized individuals, especially non-district employees
- providing access to unauthorized system programs to students (e.g. PowerSchool)
- deliberately tampering with a computer system (e.g. disabling computer hardware, deliberate virus introduction)
- theft or vandalism of any mobile device, computer, printer, network, electronic, server, computer accessories, etc.
- using the computer to tamper with, change, or alter records or documents of the district
- using restricted computer equipment without authorization from building level supervisory or district administration
- using computers which are school or district property for product advertisement or political lobbying
- using public domain software and shareware beyond the provided evaluation period without properly registering and paying for same
- use of the Internet to transmit any material that is in violation of District Five board policy and including the staff conduct policies (GBE, GBEA, GBEB, and GBEBB)

Web Publishing

District Five offers teachers and staff the ability to post information on the Internet. The purpose of this service is to promote teaching and learning. All users of Web publishing resources must adhere to the following guidelines.

- Publish only information related to official school and district business.
- Adhere to all regulations set forth in federal, state, and local laws.
- Fully comply with the permissions for each student found on the student's media consent form.
- Include contact information (preferably district e-mail addresses) on all published information.
- Never publish student contact information. This includes, but is not limited to, phone numbers, home addresses, and e-mail addresses.
- No advertising or solicitation of business unless authorized by district administration.

Confidential Information

Although the district Internet systems have security mechanisms in place, there is no way to ensure total security of the district's system. Confidential information should only be sent via the Internet on secure websites represented by (HTTPS:). District Five does not accept liability for any lost or stolen information sent or received via the district's Internet resources.

Online Behavior

Each school will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and chat rooms and cyber bullying awareness and response.

Off-Campus Conduct

Students, parents/legal guardians, teachers, and staff members should be aware that the district may take disciplinary actions for conduct initiated and/or created off-campus involving the inappropriate use of the Internet or web-based resources if such conduct poses a threat or substantially interferes with or disrupts the work and discipline of the schools, including discipline for student harassment and bullying. Staff and students must comply with all appropriate policies and including staff conduct policies (GBE, GBEA, GBEB and GBEBB).

Responsibility

District Five makes no warranties of any kind for the technology resources it is providing. The district will not be responsible for any damages the user incurs. This includes loss of data resulting from delays, non-deliveries, or incorrect deliveries of information or interruptions in technology services. Use of any information obtained via the district's technology resources is at the user's own risk. District Five specifically denies any responsibility for the accuracy, quality, or cost of information, goods, or services obtained through the district's technology services.

Employees

Administrators, teachers, and support staff may use technology resources for educational and/or work related purposes at any time which is not disruptive and does not interfere with the performance of other responsibilities by the employee or other staff members. All employees must set a good example for proper system use. All employees must observe security restrictions and make every effort to ensure that students are not using systems improperly or without authorization. In the event a user feels he/she can identify a security problem, he/she must notify the district's technology services department. Failure to notify the technology office of security problems may result in administrative or disciplinary action(s) (See staff conduct policies GBE, GBEA, GBEB and GBEBB).

Students

All District Five students will be supervised by teachers and staff in their use of District Five technology resources during school hours. Students must adhere to all of the guidelines set forth in this policy, all stipulations of technology use as outlined in the student acceptable use policy, all requirements outlined in the student disciplinary code and any school specific guidelines.

Network and Email Use Policy

This information establishes the basic structure for the use and retention of network and email resources. The use of the District Five's network and email resources will allow the district to acquire the benefits of increased efficiency through the use of technology while protecting the district's information assets, the instructional and operational integrity of the district, and the rights of students and district employees.

This policy applies to the following entities.

- all the district's employees
- all students enrolled in schools located within the district
- all other users of any of the district's technology resources, regardless of their affiliation
- all district-owned or operated technology systems which are subscribed to and/or paid by the district

Use of network and email accounts

Network and email accounts are provided by District Five as a communication resource for conducting official district business. Users of the district system must use this resource in a responsible, effective, and lawful manner.

- All messages and electronic transmissions distributed via the school district's email system are the property of District Five. The district reserves the right to monitor personal use of email to the same extent that it monitors business use. There are no expectations of privacy in any item created, stored, sent, or received on the District Five email system.
- Employees should exercise the same restraint and caution in drafting and transmitting email messages as when writing a formal memorandum on district or school letterhead. Users should assume that messages will be saved and reviewed by someone other than the original addressee.
- Although email seems to be less formal than other written communication, the same federal, state, and local laws apply to

email that apply to written communications.

If any user disregards the rules set out in this plan, the user will be fully liable for all damages incurred as a result of misuse.

Eligibility for network and email accounts

- All full-time faculty and staff and designated part-time staff will be assigned a network and email account.
- All school resource officers will be given a district network and email account.
- All state mental health workers who are assigned to District Five will be given a district network and email account.
- Long-term substitutes with a job assignment of 90 school days or more will be assigned a district network and email account upon approval from the human resources department. These accounts will expire once the job assignment is complete and all data will be deleted.
- Non-district employees are not issued a district network or email account. An example of this would be a contractor working in a school, non-district after school program personnel or temporary employee.

Acceptable use

All recipients of district network and email accounts must adhere to the following guidelines.

- Accounts cannot be used to send or forward emails containing libelous, defamatory, offensive, racist, or obscene remarks.
- Accounts cannot be used to send solicitations that are not related to official school business.
- Accounts cannot be used to disguise or attempt to disguise the user's identity when sending email or communicating via the network.
- Account bearers may not use email to consume system resources beyond a reasonable margin (for example, selling personal items or to promote a non-district related event).
- The district's network or email system will not be used to set up or run a personal business.
- Accounts cannot be used for any use that will be in conflict or violation of local, state, and/or federal laws.

Account restriction/temporary closure

- The district can restrict an employee's use of the email system without warning or notice.
- The district can temporarily deny any employee use of the email system.

Account deletion

Accounts will be disabled upon notification from the human resources department. If the account is disabled for 30 or more days, the network and email accounts and all contents from both will be deleted from the system. No person may retain a district email after termination of employment.

Mailbox retention

All users will have a usable limit of total email space on the email server. When 90 percent of the user mailbox space is filled, the user will receive an automatic notification that he/she is reaching the limit amount. Once users receive this notification they will need to remove unwanted or old email from the system. Users will be limited to 25 megabyte email attachments coming into and sending out from the district. Any attachments larger than 25 megabytes will be blocked by the system and the user will be notified.

All users are encouraged to file or archive mail that is needed beyond one school year.

Email attachments being sent into the district with files extensions of .exe, .bat, .pif, .scr will be blocked due to virus/security concerns.

Note: *The district reserves the right to retain email electronic records for one calendar year with no reasonable expectation of electronic email records being accessible or recoverable beyond this period of time, due to server space limitations and cost to maintain.*

Adopted 1/22/07; Revised 2/11/13, 2/24/14

