

Georgetown-Ridge Farm CUSD #4 Technology Acceptable Use Policy

A. Please Read

Please read this document carefully before signing. The signatures at the end of this document are legally binding and indicate that you have read this Technology Acceptable Use Policy (TAUP) and understand its significance. The failure of any user to follow the terms of the TAUP may result in the loss of privileges, disciplinary action, and/or appropriate legal action. All faculty and staff, and each student and his or her parent(s)/guardian(s) must sign the TAUP before being allowed to utilize the school's technology resources. The TAUP need only be submitted once while enrolled at Georgetown-Ridge Farm CUSD #4.

B. It's a Guide to Acceptable Technology Usage

The TAUP is intended to be a usable guide to the proper use of technology in the district. It is not intended, nor can it be, a comprehensive guide. However, some specific examples are provided to illustrate acceptable use. In summary, 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.

C. All District, Personal, Current and Future Technology Services and Equipment in the School

The TAUP will apply to both school equipment and personal technology equipment used in or on school property. This will include computers, notebook computers, personal data assistants (PDA), USB devices such as flash drives or external hard drives, memory cards, digital cameras, cellular telephones, cell cameras, MP3 players, and any wireless access devices. Any new technologies not mentioned by name in this document will also be covered by these policies.

D. Purpose

Georgetown-Ridge Farm CUSD #4 supports the acceptable and beneficial use of technology, the Internet and other computer networks in the district's instructional program in order to facilitate teaching and learning consistent with the curriculum adopted by the board. In these contexts, the board recognizes the increasing relevance of technology in the classroom. It is also necessary for students to build competency in technology to achieve postsecondary and/or professional success.

E. General Concepts

1. Students and staff are to treat all equipment with care and are to report instances of abuse or misuse as soon as the user becomes aware of the issue.
2. The school's equipment, computer network and access to the Internet are the property of the School District, and utilization of these resources is a privilege, not a right.
3. In furtherance of the purposes outlined, the district reserves the right to implement appropriate action that includes, but is not limited to, the following:
 - a. Limitation or cancellation of these privileges
 - b. Disciplinary action and/or legal action
 - c. Routine inspection of the contents of any transmissions that utilize these resources within current legal parameters
 - d. Log network use and to monitor fileserver space utilization by district users.
 - e. Other restrictions or sanctions as necessary
4. The Building Principal, and/or his/her designee will make all decisions regarding whether or not a student user has violated the TAUP and may deny, revoke, or suspend access at any time.
5. The Superintendent and/or his/her designee will make all decisions regarding whether or not a staff member has violated the TAUP and may deny, revoke, or suspend access at any time.

6. The district shall not be responsible for any information that may be lost, damaged or unavailable when using technology resources or for any information that is retrieved via the Internet.
7. The school district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

F. General Usage

The use of these devices will be at the discretion of the classroom teacher.

1. Students must obtain teacher permission before using the device in class.
2. Students will turn off and put away a device when requested by a teacher.
3. Students will not use their personal laptop outside of the classroom.
4. Students found in violation of this policy may have their device confiscated, subject to teacher discretion.
 - a. Policies regarding confiscated devices will apply as outlined in the student handbook.

G. Privacy and Access Guidelines

1. Network accounts will be used only by the authorized owner of the account for its authorized purpose.
2. Unless otherwise noted, all communications and information that are accessible via technology resources should be assumed to be private property of the district and shall not be disclosed to anyone without the written permission of the district or in accordance with current state and federal law.
3. Network users shall respect the privacy of other users on the system.

H. No Expectation of Privacy with Respect to School email or Technology Resource Usage

1. Electronic mail (email) that is processed via the school's technology resources is not private. The district technology staff has access to all email, and they are authorized to periodically monitor Internet and school email usage.
2. Teachers, students and staff possess no expectation of privacy with respect to their email or internet usage processed through the school network.
3. In addition to previously mentioned access, the district reserves the right to search otherwise private electronic records in those instances when they have reasonable suspicion that a violation of the law or school rules has occurred or where the safety of the school community is in question consistent with current legal precedents.

I. Physical Security

Users should take the following physical security preventative measures. Personal technology equipment should not be:

1. Left unattended at any time (If personal technology equipment is left unattended it will be picked up by staff and turned into building administration).
2. Left in view in an unattended vehicle

No student shall knowingly gain access to, or attempt to gain access to, any computer, computer system, computer network, information storage media, or peripheral equipment without the consent of authorized school personnel.

J. Expected Behaviors Responsible Technology Use

1. Students and staff are expected to act in a responsible, ethical and legal manner in accordance with district policy, accepted rules of technology etiquette, and federal and State law.
2. The school community will help students to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.
3. Any person who has knowledge of technology abuse or misuse has a responsibility to report it to the appropriate school personnel.
4. Any technology user who receives threatening or unwelcome communications should immediately bring them to the attention of a teacher or administrator.

5. Technology users should never reveal personal addresses, telephone numbers or other identifying information to people they do not know.

K. Examples of Prohibited Behaviors

This TAUP prohibits the use of technology resources:

1. To facilitate activities that are illegal or contrary to school rules or policies.
2. For commercial or for profit purposes.
3. For non-work or non-school related work.
4. For product advertisement or political lobbying.
5. For searching for, accessing, submitting, posting, publishing, downloading or displaying inappropriate materials by means of the Internet and/or email, blogs, web pages and social sites. This would include discriminatory remarks, and offensive or inflammatory communication including inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material. In addition, users may not search for, access, submit, post, publish download or display information by means of the Internet and/or email containing any of the following topics (unless the topic is an appropriate research assignment authorized by or conducted by a teacher):

Alcohol	Satanic Themes and/or Cults
Bomb making	Violence or Weapons
Deviant social behavior	
Gambling	
Gangs	
Human or animal mutilation	
Illegal activity	
Illegal drugs	
Libelous or Slanderous material	
Militants and/or Extremist Students or Groups	
Pornography and/or Sexually Oriented material	
Profanity	
Racism	

6. To transmit material likely to be offensive or objectionable to recipients.
7. For unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
8. To intentionally obtain or modify files, passwords, and data belonging to other users.
9. To impersonate or represent another user. This includes the use of pseudonyms.
10. To load or use unauthorized games, programs, files, or other media.
11. To disrupt the work of other users.
12. To destroy, modify or abuse hardware and software.
13. To quote personal communications in a public forum without the original author's prior consent.
14. To waste resources, such as disk space or printer supplies.
15. To gain unauthorized access to resources or entities.
16. To use technology resources while access privileges are suspended or revoked.
17. To attempt to bypass technology resource security, filters, and firewalls including the use of a proxy server.
18. Failing to exit the Internet, shutdown, or log off a computer after being instructed to do so by school personnel.
19. To harass or stalk another person by means of the Internet or email.
20. Transmitting personal information to an Internet "stranger."
21. Posting or transmitting anonymous messages.
22. To post or transmit material created by another person without authorization.

This is not all inclusive. Any other misuse of the Internet or the district's electronic network system or other electronic mediums, deemed inappropriate by school personnel, may result in disciplinary action and/or appropriate legal action.

L. Password Security

The system's security is protected through the use of passwords and monitoring software. Failure to

adequately protect or update passwords could result in unauthorized access to personal or district files. In addition, the district employs security and monitoring software to track network usage, troubleshoot problems, monitor appropriate use of technology, and restrict Internet access when needed. In addition to these efforts, the following 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 another student's or teacher'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 technology resources.
4. Any user who identifies a security issue on the Internet or Network must notify the Building Principal or System Administrator immediately. Users may not demonstrate the problem to other users.
5. Attempts to log on to technology resources as a system administrator will result in cancellation of user privileges.

M. Possible Consequences for Inappropriate Use

1. The network user shall be responsible for damages to equipment, systems, and software resulting from deliberate or willful acts.
2. Illegal use of technology resources; intentional deletion or damage to files of data belonging to others; copyrighting violations or theft of services will be reported to the appropriate legal authorities for possible prosecution.
3. General rules and policies for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use.
4. Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks. This includes but is not limited to the uploading or creation of computer viruses.
5. In the event that any user vandalizes any district computer hardware or software, he/she or the legal parent/guardian, if the user is a minor, will be responsible to pay all repair and/or replacement costs. By signing this agreement, the user and/or parent/guardian expressly agrees to be responsible for payment of costs incurred.
6. Any user, who damages, destroys, or copies another person's data will be referred for appropriate discipline and may be suspended from or denied access to all computers. Incidents in which a student copies another student's data will be treated as cheating.
7. Any user who tampers with or attempts to gain access to computer data to which he/she has no security authorization is in violation of district policy. It will be considered equivalent to tampering with a teacher's written records or attempted to gain access to confidential student information.
8. Any student who loses his/her computer use privileges due to a violation of this policy will have their academic program modified in order to accommodate their restricted technology usage.
9. The user expressly agrees to indemnify the School District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District relating to, or arising out of, any breach of this TAUP.

N. Cyber Bullying Defined

It is important to differentiate bullying from other student behaviors, "the bullying behavior includes an imbalance of power between the perpetrator and the target, is intentionally harmful, and occurs repetitively" (Olweus et al., 1999).

O. Cyber Bullying Prohibited Examples

As with the previous examples of prohibited behaviors, this list is not all inclusive.

The examples below have been provided by the Illinois Attorney General's office, and may be found at the following website: http://illinoisattorneygeneral.gov/cyberbullying/FormsOfCyberbullying_0108.pdf.

1. Chat Rooms: Sending a mean or threatening message to be viewed by everyone in a chat room.

2. IMing/Text Messaging/Emailing: Sending a mean or threatening message. This may include forwarding an email without the original sender's permission.
3. Stealing Passwords: Using another person's account or cell phone without authorization to send mean or threatening messages.
4. Impersonation: Using the internet or cell phone to pretend to be someone else and sending mean or threatening messages.
5. Blogging/Bash Boarding: Posting mean or hurtful content about someone in a public forum.
6. Web Sites: Participating in an existing Web site or the creation of a Web site with the purpose of degrading, humiliating, harassing, or threatening another person. This can include Web sites that rate how someone looks or bash someone's race or sexual orientation.
7. Sending Pictures: Sending, posting, or altering compromising pictures of others whether the images were taken with or without consent.
8. Sending Spyware and/or Hacking Programs: Using technology to jeopardize or gain unauthorized access to someone else's computer.

P. Cyber Bullying Acceptable Student Responses

Not every incident of student conflict will result in school related discipline. Some instances may require intervention through outside authorities. This list is also provided by the Illinois Attorney General's office, and may be found at the following website:

http://illinoisattorneygeneral.gov/cyberbullying/Responding2Cyberbully_students__0108.pdf.

1. Print out all instances of cyber bullying.
2. Preserve electronic evidence. If you receive a mean or threatening message, do not delete the message. You should take a screenshot of the message or store the message in a folder. There may be important electronic information that can help law enforcement trace the source.
3. Report improper content and usage to the perpetrator's website or Internet Service Provider (e.g., comcast or at&t). Most websites and Internet service providers have a terms of service agreement that prohibits members from using their service to harass or threaten others. Most websites and Internet service providers also supply a link to report this type of abuse.
4. Ignore the sender. You do not have to respond. In fact, responding can escalate the situation.
5. Block the sender. If ignoring the person does not improve the situation, you can call you phone company and ask them to block the number so that the person can no longer call your phone. You can also remove a person from a buddy list.
6. Tell a trusted adult (parent, teacher, social worker, or law enforcement).
7. If you feel you are in danger, call 911 immediately.

Student Acknowledgement (Required for Students in Grades 3-12)

I have read, understand and agree to abide by the rules set forth in the above Technology Acceptable Use Policy. I further understand that should I commit any violation, my access privileges may be revoked and disciplinary action and/or appropriate legal action may be taken. I understand that access to technology is for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to fully restrict access to all controversial and inappropriate materials and maintain a beneficial learning tool. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by technology resources.

Student Printed Name

Student Signature

Date: _____

Parent/Guardian Acknowledgement

I have read, understand and agree to abide by the rules set forth in the above Technology Acceptable Use Policy. I have discussed the terms of the agreement with my son/daughter. I understand that access to technology is for educational purposes, and that the District has taken all reasonable precautions to block access to inappropriate materials from school websites. However, I also recognize it is impossible for the District to fully restrict access to all controversial and inappropriate materials and maintain a beneficial learning tool. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by technology resources. I further accept full responsibility for the supervision of my child’s technology use outside the school setting. I have discussed the terms of this Technology Acceptable Use Policy with my child, and I hereby request that my child be allowed access to the district’s technology resources.

Parent/Guardian Printed Name

Parent/Guardian Signature

Date: _____

Staff Acknowledgement

I have read, understand and agree to abide by the rules set forth in the above Technology Acceptable Use Policy. I further understand that should I commit any violation, my access privileges may be revoked and disciplinary action and/or appropriate legal action may be taken. I understand that access to technology is for educational purposes and that the District has taken precautions to eliminate controversial material. However, I also recognize it is impossible for the District to fully restrict access to all controversial and inappropriate materials and maintain a beneficial learning tool. I will hold harmless the District, its employees, agents, or Board members, for any harm caused by technology resources.

Staff Printed Name

Staff Signature