Palestine ISD Employees Handbook

Technology Responsible Use Guideline (RUG)

Personal Use of Electronic Media

Electronic media includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), Web logs (blogs), electronic forums (chat rooms), video-sharing Web sites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g. Facebook, MySpace, Twitter, LinkedIn). Electronic media also includes all forms of telecommunication such as landlines, cell phones, and Web-based applications. As role models for the district's students, employees are responsible for their public conduct even when they are not acting as district employees. Employees will be held to the same professional standards in their public use of electronic media as they are for any other public conduct. If an employee's use of electronic media interferes with the employee's ability to effectively perform his or her job duties; the employee is subject to disciplinary action, up to and including termination of employment. If an employee wishes to use a social network site or similar media for personal purposes, the employee is responsible for the content on the employee's page, including content added by the employee, the employee's friends, or members of the public who can access the employee's page, and for Web links on the employee's page, The employee is also responsible for maintaining privacy settings appropriate to the content.

An employee who uses electronic media for personal purposes shall observe the following:

- The employee may not set up or update the employee's personal social network page(s) using the district computers, network, or equipment.
- The employee shall not use the district's logo or other copyrighted material of the district without express, written consent.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators, even when communicating regarding personal and private matters, regardless of whether the employee is using private or public equipment, on or off campus. These restrictions include:
    - Confidentiality of student records.
    - Confidentiality of health or personnel information concerning colleagues, unless disclosures serves lawful professional purposes or is required by law.
    - Confidentiality of district records, including educator evaluations and private e-mail.

- Copyright law.
- Prohibition against harming others by knowingly making false statements about a colleague or the school system.

See ***Use of Electronic Media with Students*** below for regulations on employee communication with students through electronic media.

Technology Resources

The district's technology resources, including its network access to the Internet, are primarily for administrative and instructional purposes. Limited personal use is permitted if the use:

- Imposes no tangible cost to the district
- Does not unduly burden the district's technology resources
- Has no adverse effect on job performance or on a student's academic performance

Electronic mail transmissions and other use of technology resources are not confidential and can be monitored at any time to ensure appropriate use,

Employees who are authorized to use the systems are required to abide by the provisions of the district's acceptable use guideline and administrative procedures. Failure to do so can result in suspension of access or termination of privileges and may lead to disciplinary action. Employees with questions about computer use and data management can contact the Technology Department at (903) 731-8003.

Use of Electronic Media with Students

A certified or licensed employee, or any other employee designated in writing by the superintendent or a campus principal, may communicate through electronic media with students who are currently enrolled in the district. The employee must comply with the provisions outlined below. All other employees are prohibited from communicating with students who are enrolled in the district through electronic media.

An employee is not subject to these provisions to the extent the employee has a social or family relationship with a student. For example, an employee may have a relationship with a niece or nephew, a student who is the child of an adult friend, a student who is a friend of the employee's child, or a member or participant in the same civic, social, recreational, or religious organization.

The following definitions apply for the use of electronic media with students:

- ***Electronic media*** includes all forms of social media, such as text messaging, instant messaging, electronic mail (e-mail), Web logs (blogs), electronic forums (chat rooms), video-sharing Web sites (e.g., YouTube), editorial comments posted on the Internet, and social network sites (e.g., Facebook, MySpace, Twitter, and Linkedln).

Electronic media also includes all forms of telecommunication such as land lines, cell phones, and Web-based applications.

- ***Communicate*** means to convey information and includes a one-way communication as well as a dialogue between two or more people. A public communication by an employee that is not targeted at students (e.g., a posting on the employee's personal social network page or a blog) is not a communication; however, the employee may be subject to district regulations on personal electronic communications. See Personal Use of Electronic Media, above. Unsolicited contact from a student through electronic means is not a communication.

- ***Certified or licensed employee*** means a person employed in a position requiring SBEC certification or a professional license, and whose job duties may require the employee to communicate electronically with students.

The term includes classroom teachers, counselors, principals, librarians, paraprofessionals, nurses, educational diagnosticians, licensed therapists, and athletic trainers.

An employee who uses electronic media to communicate with students shall observe the following:

- The employee may use any form of electronic media except text messaging. Only a teacher, trainer, or other employee who has an extracurricular duty may use text messaging, and then only to communicate with students who participate in the extracurricular activity over which the employee has responsibility.

- The employee shall limit communications to matters within the scope of the employee's professional responsibilities (e.g., for classroom teachers, matters relating to class work, homework, and tests; for an employee with an extracurricular duty, matters relating to the extracurricular activity. The employee is prohibited from knowingly communicating with students through a personal social network page; the employee must create a separate social network page ("professional page") for the purpose of communicating with students. The employee must enable administration and parents to access the employee's professional page.

- The employee shall not communicate directly with any student between the hours of 10:00 p.m. and 7:00 a.m. An employee may, however, make public posts to a social network site, blog, or similar application at any time.

- The employee does not have a right to privacy with respect to communications with students and parents.
- The employee continues to be subject to applicable state and federal laws, local policies, administrative regulations, and the Code of Ethics and Standard Practices for Texas Educators, including:
    - ❖ Compliance with the Public Information Act and the Family Educational Rights and Privacy Act (FERPA), including retention and confidentiality of student records.
- Prohibitions against soliciting or engaging in sexual conduct or a romantic relationship with a student.
- Upon request from administration, an employee will provide the phone number(s), social network site(s), or other information regarding the method(s) of electronic media the employee uses to communicate with anyone or more currently-enrolled students.
- Upon written request from a parent or student, the employee shall discontinue communicating with the student through e-mail, text messaging, instant messaging, or any other form of one-to-one communication.

An employee may request an exception from one or more of the limitations above by submitting a **written** request to his or her immediate supervisor.

Electronic Communications Terms and Conditions

Responsible Use - The purpose of providing electronic communications is to support education and research by providing access to unique resources and the opportunity for collaborative work. The use of your account must be in support of education and research and consistent with the educational objectives of the Palestine Independent School District. Use of electronic resources must comply with the rules appropriate for that resource. Transmission of material in violation of U.S. or State regulations is prohibited. This includes, but is not limited to copyrighted material, threatening or obscene material, pornography, or material protected by trade secret. Also prohibited are illegal access to computers or networks ("hacking"), commercial activities, product advertisement, personal advertising, chain letters, and political lobbying.

Privileges - The use of electronic communications is a privilege, not a right, and inappropriate use may result in a cancellation or restriction of those privileges. Each person who receives an account or uses District network resources agrees to the terms and conditions of the Electronic Communications Policy. All electronic communications, including, but not limited to, e-mail,

Internet activity and network resources may be monitored at any time by the system administrators.

No electronic communications activity using District resources is considered private. The system administrators will routinely perform maintenance and monitoring of the system that may lead to the discovery that a user has violated guideline or law. Additionally, an individualized search will be conducted if there is reasonable suspicion that a user has violated a guideline or law.

Inappropriate use of electronic communications, including "hacking," constitutes as a disciplinary offense for employees and will be dealt with according to District policy.

District employees shall be governed by the Standards of Conduct outlined in the Employee Handbook. Activities in violation of state or federal laws will be reported to the appropriate authorities. The system administrators will deem what is inappropriate use. Also, the system administrators may close an account at any time as required. The administration, faculty and staff of Palestine Independent School District may request the system administrator to deny, revoke or suspend specific user accounts.

Network Etiquette - Users are expected to abide by the generally-accepted rules of network etiquette. These include (but are not limited to) the following:

1. Be polite. Do not get abusive in messages to others.

2. Use appropriate language. Do not swear, use vulgarities or any other inappropriate language, as accepted by community standards. Illegal activities are strictly forbidden.

3. Do not reveal personal addresses or phone numbers or those of students or colleagues.

4. Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities will be reported to the authorities.

5. Do not use electronic resources in such a way that would disrupt their use by others.

6. Do not attempt to gain access to locations on networks where specific privileges have not been given.

7. All communications and information accessible via electronic communications should be assumed to be copyrighted unless otherwise stated.

Warranties - Palestine Independent School District makes no warranties of any kind, whether expressed or implied, for the service it is providing. Palestine Independent School District will not be responsible for any damages. This includes loss of data resulting from delay, non-delivery, mis-delivery, or service interruption caused by the District's own negligence or user errors or omissions. Use of any information obtained via the Internet is at user's own risk.

Palestine Independent School District specifically denies any responsibility for the accuracy or quality of information obtained through the network.

Security - Security on any computer system is a high priority, especially when the system involves many users. If a user can identify a security problem on the network, the user must notify a system administrator. Do not demonstrate the problem to other users. Do not use another individual's account without written permission from that individual. Attempts to log on to the network as another user will result in cancellation of user privileges. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network. All computers can be monitored at any time by the Technology Department.

Purchases - Users are solely responsible for services, memberships or merchandise purchased through the District's access to electronic communications. The Palestine Independent School District shall not be a party to such transactions or be liable for any costs or damages arising out of, either directly or indirectly, such actions.

Vandalism - Vandalism will result in cancellation of privileges. Vandalism is defined as any malicious attempt to harm or destroy equipment or data of another user, the network, or through electronic communications. This includes, but is not limited to, uploading or creating computer viruses, gaining illegal access to a computer or network or altering electronic information belonging to others.

Damages - The user specifically agrees to reimburse the Palestine Independent School District and the system administrators for any losses, costs, or damages, including reasonable attorneys' fees incurred by the Palestine Independent School District and the system administrators relating to, or arising out of any breach of the electronic communications guideline by the user.

Antivirus Software - A computer virus is a malicious program that can attach itself to executable files and operating system files on both floppy and hard disks. Viruses can destroy data and in some cases damage hardware. Viruses are spread by sharing files, disks, and by downloading programs from the Internet or E-mail. Antivirus software is provided for every computer on the Palestine Independent School District's network. This software must not be disabled or tampered with by the user. Virus attacks should be reported to the Technology Department or the Help Desk. Intentionally introducing or spreading a virus will be considered vandalism and will result in the cancellation of privileges.

Laptop Computers - Laptop computers, which were not purchased by the Palestine Independent School District, may not be connected to the District's network or phone lines without the express permission of the Director of Technology.

Care and security of the PISD laptops assigned to the employee is the direct responsibility of the employee. The employee must report damaged technology equipment to the PISD Technology Department immediately. Any lost or stolen technology equipment must be reported to the

Palestine Police Department immediately. Any cost of repair or replacement of technology equipment due to obvious employee negligence will be debited from the employee's paycheck.

All equipment, including laptops assigned to the employee, is to be returned to the District facility from which it was assigned within 24 hours of the employee being reassigned to another facility or upon termination of employment. Any equipment not returned will have its total replacement cost debited from the employee's last paycheck.

I acknowledge receipt of the above guideline. (Please sign)

_____

Date _____

Palestine I.S.D. Student Handbook -

Responsible Use Guideline (RUG) for Technology

BULLYING/CYBERBULLYING

Students are not allowed to threaten or harass other students in any manner. Students may be disciplined for threats made outside of school if the threat causes material or substantial disruption at school, including, but not limited to, the following:

- Communicating oral or written threats to cause harm or bodily injury to another student, district employee, official, volunteer, or school property, including threats made using the Internet or other computer resources at school.
- Sending or posting electronic messages that are abusive, obscene, sexually oriented, harassing, or illegal.
- Violating policies or rules for computer use or Internet access.
- Transmitting/displaying material that is sexually oriented, pornographic, obscene, or reveals a person's private body parts.

ELECTRONIC COMMUNICATIONS DEVICES

The district prohibits students from using electronic communication devices without permission at school during the instructional day and lunch. The instructional day is determined by the Principal. Electronic communication devices include but are not limited to:

Portable telephones (including cellular, digital, camera, Internet capable, etc.) two- way radios, pagers, beepers. Any other electronic device capable of transmitting electronic signals (including: Bluetooth and/or infrared technology, IPods, MP3 players, handheld games, Blackberries, Smartphones, etc.)

Students may possess electronic communication devices at school; however, such devices, including accessories for such devices, shall not be visible and shall remain off during the school day. Students may use PDA's (Personal Digital Assistants) during the school day with the permission of the classroom teacher for instructional purposes only. To help ensure the testing environment is not compromised, schools may impose different rules for possession of electronic communication devices on days that statewide assessments or district benchmark tests are administered.

A student violates this guideline if the electronic communication device is either visible and/or turned on without the express permission of a school official. A violation of this policy will result in the confiscation of the device. The device will be returned to the student upon payment of a $15.00 administrative fee. Repeated violations of this guideline can result in the administrator request of a parent conference/pickup or confiscation of the phone for the remainder of the semester or school year. Students who use their cell phones to record inappropriate behavior at school may lose the right to bring cell phones to school.

The district expects that parents will promptly retrieve electronic communication devices confiscated under this guideline. The district is not responsible for theft, damage, or loss of such confiscated devices. Any devices not retrieved by noon on the last school day of the semester in which the device is confiscated will not be returned and will be forwarded to District administration for disposal.

MISUSE OF TECHNOLOGY RESOURCES AND THE INTERNET

Students shall not:

- Violate policies, rules, or agreements signed by the student and/or agreements signed by the student's parent/guardian regarding the use of technology resources.
- Attempt to access or circumvent passwords or other security-related information of the district, students, or employees or upload or create computer viruses, including off-school property, in order to cause a substantial disruption to the educational environment.
- Attempt to alter, destroy, or disable district technology resources including but not limited to computer equipment, district data, the data of others, or other networks connected to the district's system, including off-school property in an attempt to cause a substantial disruption to the educational environment.
- Use the Internet or other electronic communications to threaten district students, employees, or volunteers, including off school property, in an effort to cause a substantial disruption to the educational environment.

Inappropriate use of electronic communications constitutes a Level 1 offense for students, and "hacking" constitutes a Level 2 offense as outlined in the PISD Student Behavior Policy. Offenses will be dealt with according to District policy.

Palestine I.S.D. - Parent/Student Handbook

Responsible Use Guideline (RUG) for Technology

ELECTRONIC DEVICES AND TECHNOLOGY RESOURCES

Possession and Use of Personal Telecommunications Devices, Including Mobile Telephones.

The district prohibits students from using electronic communication devices without permission at school during the instructional day and lunch. The instructional day is determined by the Principal.

Electronic communication devices include but are not limited to:
Portable telephones (including cellular, digital, camera, Internet capable, etc.) two- way radios, pagers, beepers. Any other electronic device capable of transmitting electronic signals (including: Bluetooth and/or infrared technology, IPods, MP3 players, handheld games, Blackberries, Smart phones, etc.)

Students may possess electronic communication devices at school; however, such devices, including accessories for such devices, shall not be visible and shall remain off during the school day. Students may use PDA's (Personal Digital Assistants) during the school day with the permission of the classroom teacher for instructional purposes only. To help ensure the testing environment is not compromised, schools may impose different rules for possession of electronic communication devices on days that statewide assessments or district benchmark tests are administered.

A student violates this guideline if the electronic communication device is either visible and/or turned on without the express permission of a school official. A violation of this guideline will result in the confiscation of the device. The device will be returned to the student upon payment of a $15.00 administrative fee. Repeated violations of this guideline can result in the administrator's request for a parent conference/pickup. If repeated or severe violations of the cell phone use guideline continue after a parent conference, the student's privileges may be revoked permanently or long-term.

The district expects that parents will promptly retrieve electronic communication devices confiscated under this guideline. The district is not responsible for theft, damage, or loss of such confiscated devices. Any devices not retrieved by noon on the last school day of the semester in which the device is confiscated, will not be returned and will be forwarded to District administration for disposal.

Any disciplinary action will be in accordance with the Student Code of Conduct. The district will not be responsible for damaged, lost, or stolen electronic communications devices. For safety purposes, the district permits students to possess personal mobile telephones; however, these devices must remain turned off during the instructional day, including during all testing unless they are being used for approved instructional purposes. A student must have approval to possess other telecommunications devices such as netbooks, laptops, tablets, or other portable computers.

The use of mobile telephones or any device capable of capturing images is strictly prohibited in locker rooms or restroom areas while at school or at a school-related or school-sponsored event. If a student uses a telecommunications device without authorization during the school day, the device will be confiscated. The [student/parent] may pick up the confiscated telecommunications device from the principal's office for a fee of $15. Confiscated telecommunications devices that are not retrieved by the student or the student's parents will be disposed of after the notice required by law. In limited circumstances and in accordance with law, a student's personal telecommunications device may be searched by authorized personnel. Any disciplinary action will be in accordance with the Student Code of Conduct. The district will not be responsible for damaged, lost, or stolen telecommunications devices.

Instructional Use of Personal Telecommunications and Other Electronic Devices

In some cases, students may find it beneficial or might be encouraged to use personal telecommunications or other personal electronic devices for instructional purposes while on campus. Students must obtain prior approval before using personal telecommunications or other personal electronic devices for instructional use. Students must also sign a user agreement that contains applicable rules for use (separate from this handbook). When students are not using the devices for approved instructional purposes, all devices must be turned off during the instructional day. Violations of the user agreement may result in withdrawal of privileges and other disciplinary action.

Responsible Use of District Technology Resources

To prepare students for an increasingly technological society, the district has made an investment in the use of district-owned technology resources for instructional purposes; specific resources may be issued individually to students. Use of these technological resources, which include the district's network systems and use of district equipment, is restricted to approved purposes only. Students and parents will be asked to sign a user agreement (separate from this handbook) regarding use of these district resources. Violations of the user agreement may result in withdrawal of privileges and other disciplinary action.

Unacceptable and Inappropriate Use of Technology Resources

Students are prohibited from possessing, sending, forwarding, posting, accessing, or displaying electronic messages that are abusive, obscene, sexually oriented, threatening, harassing, damaging to another's reputation, or illegal. This prohibition also applies to conduct off school property, whether the equipment used to send such messages is district- owned or personally owned, if it results in a substantial disruption to the educational environment. In order to ensure that students are not practicing unacceptable and/or inappropriate uses of technology resources, in addition to its own monitoring system, Palestine ISD utilizes a Human Monitoring Service (HMS) provided by the student email provider. The HMS is constantly reviewing and monitoring student accounts to apply consistent, district-approved policies to any violations, while also keeping the District informed of such violations. Any person taking, disseminating, transferring, possessing, or sharing obscene, sexually oriented, lewd, or otherwise illegal images or other content, commonly referred to as "sexting," will be disciplined according to the Student Code of Conduct and may, in certain circumstances, be reported to law enforcement.

In addition, any student who engages in conduct that results in a breach of the district's computer security will be disciplined in accordance with the Student Code of Conduct, and, in some cases, the consequences may rise to the level of expulsion.

PISD Technology Responsible Use Guidelines (RUG) and Student Online Safety Pledge

As a STUDENT of Palestine I.S.D., I have read the District's RUG (Responsible Use Guideline) and agree to abide by its provisions. It is understood that access to the Internet, the District's Computer Network System, or District's technology is a privilege, not a right. Failure to abide by the rules in this document could result in the revocation of access privileges, disciplinary action, or legal action, as deemed appropriate. In addition, I understand that there are certain rules about what I should do online. I agree to follow these rules:

1. I will not give my name, address, telephone number, school, or my teachers'/parents' names, addresses, or telephone numbers, to anyone I meet on the Internet.
2. I will not give out my email password to anyone (even my best friends) other than my teachers/parents.
3. I will not send a picture of myself or others over the Internet without my teachers'/parents' permission.
4. I will not fill out any form or request online that asks me for any information about my school, my family, or myself without first asking for permission from my teachers/parents.
5. I will tell my teachers/parents if I see any bad language or pictures on the Internet, or if anyone makes me feel nervous or uncomfortable online.
6. I will never agree to get together with someone I "meet" online without first checking with my teachers/parents. If my teachers/parents agree to the meeting, I will be sure that it is in a public place and that I am accompanied by an adult at all times.
7. I will not use any articles, stories, or other works I find online and pretend it is my own.
8. I will not use bad language online.
9. I will practice safe computing, and check for viruses whenever I borrow a disk from someone, download something from the Internet, or receive an attachment.
10. I will be a good online citizen and not participate in any activity that hurts others or is against the law or my school's guideline.

_____ _____ _____

Student's Signature Date Grade

As the parent/guardian of _____, I have read the Palestine ISD's Technology Responsible Use Guideline (RUG). In consideration for my student's use of Palestine ISD's Internet, Computer Network System, and Technology, I hereby release Palestine ISD, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my student's use of, or inability to use, the system, including, without limitation, the type of damage identified in the Palestine ISD RUG.

___ YES, I give my student permission to participate in the District's Internet System, Network System, and/or with the District's Technology and certify information on this form is correct***. I also certify that I have gone over this information with my student and that he/she understands the consequences of violation of this guideline.***

___ NO, I do not give permission for my student to participate in the District's Internet System, Network System, and/or with the District's Technology.

_____ _____

Parent's Signature Date

_____ _____

Home Address Phone Number

The Palestine ISD does not discriminate on the basis of race, color, religion, gender, national origin, age, disability, military status, genetic information, or on any other basis prohibited by law in employment, educational programs, or activities.