

## **ROBINSON INDEPENDENT SCHOOL DISTRICT ACCEPTABLE USE POLICY (AUP)**

The Superintendent or designee will oversee the District's electronic communications system.

The District's system will be used only for administrative and educational purposes consistent with the District's mission and goals. Commercial or political use of the District's system is strictly prohibited.

The District will provide training to employees in proper use of the system and will provide all users with copies of acceptable use guidelines. All training in the use of the District's system will emphasize the ethical use of this resource.

Copyrighted software or data may not be placed on any system connected to the District's system without permission from the holder of the copyright. Only the owner(s) or individuals the owner specifically authorizes may upload copyrighted material to the system.

### **SYSTEM ACCESS**

Access to the District's electronic communications system will be governed as follows:

1. With the approval of the immediate supervisor, District employees will be granted access to the District's system.
2. Students completing required course work on the system will have first priority for use of district equipment after school hours.
3. Any system user identified as a security risk or having violated District and/or campus computer-use guidelines may be denied access to the District's system.
4. Set limits for disk utilization on the system, as needed (home directory, email, etc.).

### **CAMPUS-LEVEL COORDINATOR RESPONSIBILITIES**

As the campus-level coordinator for the electronic communications system, the principal or designee will:

1. Be responsible for disseminating and enforcing applicable District policies and acceptable use guidelines for the District's system at the campus level.
2. Ensure that all users of the District's system complete and sign an agreement to abide by District policies and administrative regulations regarding such use. All such agreements will be maintained on file in the principal's office.
3. Ensure that employees supervising students who use the District's system provide training emphasizing the appropriate use of this resource.
4. Be authorized to monitor or examine all system activities, including electronic mail transmissions, as deemed appropriate to ensure proper use of the system.
5. Be authorized to establish a retention schedule for messages on any electronic bulletin board and to remove messages posted locally that are deemed to be inappropriate.

## **INDIVIDUAL USER RESPONSIBILITIES**

The following standards will apply to all users of the District's electronic information/communications systems:

### **ON-LINE CONDUCT**

1. The individual in whose name a system account is issued will be responsible at all times for its proper use.
2. The system may not be used for illegal purposes, in support of illegal activities, or for any other activity prohibited by District policy.
3. System users may not use another person's system account without permission from District coordinator, as appropriate.
4. System users must purge electronic mail in accordance with established retention guidelines.
5. System users may redistribute copyrighted programs or data **only with** the written permission of the copyright holder or designee. Such permission must be specified in the document or must be obtained directly from the copyright holder or designee in accordance with applicable copyright laws, District policy, and administrative regulations.
6. System users may upload public domain programs to the system. System users may also download public domain programs for their own use or may non-commercially redistribute a public domain program. System users are responsible for determining whether a program is in the public domain.
7. UNDER NO CIRCUMSTANCES is a student or your child allowed on a teacher workstation. And staff children are not allowed on any machine after school hours without staff supervision. Violations of this policy will result in the immediate loss of computer access for that teacher.

### **VANDALISM PROHIBITED**

Any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's system, or any the agencies or other networks that are connected to the Internet is prohibited. Deliberate attempts to degrade or disrupt system performance may be viewed as violations of District policy and administrative regulations and, possibly, as criminal activity under applicable state and federal laws. This includes, but is not limited to, the uploading or creating of computer viruses.

Vandalism as defined above will result in the cancellation of system use privileges and will require restitution for costs associated with system restoration, hardware, or software costs.

### **FORGERY PROHIBITED**

Forgery or attempted forgery of electronic mail messages is prohibited. Attempts to read, delete, copy, or modify the electronic mail of other system users or deliberate interference with the ability of other system users to send/receive electronic mail is prohibited.

## **INFORMATION CONTENT/THIRD PARTY SUPPLIED INFORMATION**

System users and parents of students with access to the District's system should be aware that use of the system may provide access to other electronic communications systems in the global electronic network that may contain inaccurate and/or objectionable material. A student knowingly bringing prohibited materials into the school's electronic environment will be subject to a suspension and/or a revocation of privileges on the District's system and will be subject to disciplinary action in accordance with the Student Code of Conduct. An employee knowingly bringing prohibited materials into the school's electronic environment will be subject to disciplinary action in accordance with District policies.

## **NETWORK ETIQUETTE**

System users are expected to observe the following network etiquette:

1. Be polite; messages typed in capital letters are the computer equivalent of shouting and are considered rude.
2. Use appropriate language; swearing, vulgarity, ethnic or racial slurs, and any other inflammatory language are prohibited.
3. Pretending to be someone else when sending/receiving messages is considered inappropriate.
4. Posting or distribution of messages or pictures that are obscene, vulgar, profane, sexually oriented, pornographic, highly offensive to others, highly threatening to others, or illegal is prohibited.
5. Revealing personal addresses or phone numbers of the user or others is prohibited.
6. Using the network in such a way that would disrupt the use of the network by other users is prohibited.
7. "Hacking," i.e., attempting unauthorized access to any computer whether within the district's network or outside it.

## **TERMINATION/REVOCAION OF SYSTEM USER ACCOUNT**

The District may suspend or revoke a system user's access to the District's system upon violation of District policy and/or administrative regulations regarding acceptable use. Termination of an employee's account or of a student's access will be effective on the date the principal or District coordinator receives notice of student withdrawal or of revocation of system privileges, or on a future date if so specified in the notice.

**DISCLAIMER** The District's system is provided on an "as is, as available" basis. The District does not make any warranties, whether express or implied, including, without limitation, those of merchantability and fitness for a particular purpose with respect to any services provided by the system and any information or software contained therein. The District does not warrant that the functions or services performed by, or that the information or software contained on, the system will meet the system user's requirements, or that the system will be uninterrupted or error-free, or that defects will be corrected. Opinions, advice, services, and all other Information expressed by system users, information providers, service providers, or other third party individuals in the system are those of the providers and not the District. The District will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the District's electronic communications system.

## **Bring Your Own Device (BYOD)**

1. Robinson ISD is planning to implement a "Bring Your Own Device" pilot program in the 2012-2013 school year. We plan to begin with the high school campus. Your student may be included in the initial stages of this program.
2. Robinson ISD uses Instructional Technology as one way of enhancing the mission to teach the skills, knowledge and behaviors students will need as responsible citizens in the global community. Students learn collaboration, communication, creativity and critical thinking in a variety of ways throughout the school day. In an effort to increase access to those 21st century skills, Robinson ISD will allow personal devices on our network and school grounds for students who follow the responsibilities stated in the Acceptable Use Policy and the attached guidelines regarding BYOD.
3. Robinson ISD provides technology that is appropriate and adequate to support instructional purposes. The use of personal devices by students is optional, and students who do not participate in BYOD. will not be penalized and alternate modes of participation will be available.
4. An important component of BYOD will be education about appropriate online behaviors. We will offer reminders and reinforcement about safe online behaviors. In addition to the rules outlined in these guidelines, students will be expected to comply with all class and school rules while using personal devices

## **BYOD Device Type**

1. For the purpose of this program, the word "devices" will include: laptops, netbooks, ultra books, chromebooks, cell phones, smart phones, iPads, iPods, and tablets. Please note that Nintendo DS, PSP and/or other gaming devices with internet access are not permissible at this time.
2. Wireless devices only.

## **BYOD Guidelines**

1. Students and parents/guardians participating in BYOD must adhere to the Student Code of Conduct, Student Handbook, and all Board policies, particularly Robinson ISD Acceptable Use Policy.
2. Each teacher has the discretion to allow and regulate the use of personal devices in the classroom and on specific projects.
3. Approved devices must be in silent mode while riding school buses and on school campuses, unless otherwise allowed by a teacher.
4. Devices may not be used to cheat on assignments or tests, or for non-instructional purposes (such as making personal phone calls, text/instant messaging, and using social networking sites).
5. Students may not use devices to record, transmit or post-photographic images or video of a person, or persons on campus during school activities and/or hours, unless otherwise allowed by a teacher.
6. Devices may only be used to access files on computer or internet sites which are relevant to the classroom curriculum. Games are not permitted, unless otherwise allowed by a teacher.
7. The school's network filters will be applied to a device's connection to the internet and any attempt to bypass the network filters is prohibited.
8. Students are prohibited from:
  - a. Bringing a device on premises that infects the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information,

and processing or accessing information on school property related to “hacking”, altering, or bypassing network security policies.

- b. Robinson ISD is authorized to collect and examine any device that is suspected of causing technology problems or was the source of an attack or virus infection.
- c. At no time should a student or faculty connect a personal device directly to our wired network. Wireless access only is permitted.

### **BYOD Lost, Stolen, or Damaged Devices**

Each user is responsible for his/her own digital property, and should treat it and use it responsibly and appropriately, Robinson ISD takes no responsibility for stolen, lost, or damaged devices, including lost or corrupted data on those devices. While school employees will help students identify how to keep personal devices secure, students will have the final responsibility for securing their personal devices. Please check with your homeowner’s policy regarding coverage of personal electronic devices, as many insurance policies can cover loss or damage.

### **BYOD Usage Charges**

Robinson ISD cannot be held responsible for any possible device charges to your account that might be incurred during approved school-related use.

### **BYOD Network Considerations**

Users should strive to maintain appropriate bandwidth for school-related work and communications. All users will use the “RISD-BYOD” wireless network to access the internet. Robinson does not guarantee connectivity or quality of connection with personal devices, but will provide trouble-shooting documentation on how to connect with a variety of operating systems and devices.

Robinson Independent School District Employee/Student Agreement of Acceptable Use Policy

(Print the agreement, fill it out and return it to your campus office.)

I have read the District's acceptable use policy and agree to abide by their provisions. In consideration for the privilege of using the District's electronic communications system and in consideration for having access to the public networks, I hereby release the District, its operators, and any institutions with which they are affiliated from any and all claims and damages of any nature arising from my use of, or inability to use, the system, including, without limitation, the type of damages identified in the District's policy and administrative regulations.

Name (Print): \_\_\_\_\_

Signature: \_\_\_\_\_

Date: \_\_\_\_\_