

STUDENT NAME: \_\_\_\_\_ Class/Grade: \_\_\_\_\_

**RIO GRANDE SCHOOL STUDENT TECHNOLOGY  
ACCEPTABLE USE POLICY  
2011-2012 School Year**

**I. Purpose**

Rio Grande School (“RGS”) is pleased to offer students access to its computer system for educational use of the computer and Internet access under teacher supervision and discretion. The school’s computer system has become an integral part of the educational process at RGS and is used daily by students and teachers in classrooms. The objective is to provide educational experiences that allow students to develop 21<sup>st</sup> century technology skills, and to conduct research and produce projects that support grade level curriculum.

**II. Definitions**

As used herein:

- A. “User” means all persons who are granted access to RGS’ computer resources.
- B. “Computer Resources” means all computer hardware, computer software, communications devices, facilities, equipment, networks, passwords, licensing and attendant policies, manuals, and guides.
- C. “Computer System” means the computer resources, computer networks, servers, or computers owned or operated by RGS.

**III. No Expectation of Privacy**

- A. *No expectation of privacy.* The computers, computer resources, and computer accounts given to Users are to assist them in performance of their jobs or education. Users do not have an expectation of privacy in anything they create, store, send, or receive on the computers, computer resources, or computer systems of RGS. The computer system belongs to the School for business and/or educational program purposes.
- B. *Waiver of privacy rights.* Users expressly waive any right of privacy in anything they create, store, send, or receive on the computes, computer resources, or computer systems, or through the internet or any other computer network.
- C. *Supervision and Monitoring.* School and network administrators and their authorized employees monitor the use of computer resources and computer systems to help ensure that uses are secure and in conformity with this policy. Administrators reserve the right to examine, use, and disclose any data found on the School's computer systems or computer resources in order to further the health, safety, discipline, or security of any student or other person, or to protect property. They may also use this information in disciplinary actions, and will furnish evidence of crime to law enforcement.

#### **IV. Student Computer Use Expectations and Prohibitions**

A. Supervised access to RGS computer systems and computer resources is provided to students who agree to act in a considerate and responsible manner. Students are responsible for good behavior on the schools computer system just as they are in a classroom or a school hallway. To this end, Students must:

- Respect and protect the privacy of others;
- Only email from the classroom teacher's school email account. Access by students to personal email accounts is not allowed at school;
- Report any threatening, discomfoting, inappropriate, or unlawful materials to a teacher or administrator;
- Use only assigned accounts;
- Not use another's private password, or view another's private data or email to which they are not authorized;
- Not give out private information about others or themselves without teacher approval;
- Report any known acceptable use policy violations to a teacher or administrator; and
- Communicate only in ways that are kind and respectful.

B. Students are prohibited from:

- Viewing, sending by email, or otherwise transmitting or storing material that is fraudulent, harassing, embarrassing, lewd, sexually explicit, profane, obscene, intimidating, threatening or potentially violent, defamatory, racially offensive, proselytizing, inappropriate or otherwise unlawful, or in violation of School policy ("inappropriate or unlawful material"). Students encountering this kind of material should immediately report the incident to their teacher or another administrator;
- Using computer resources, computers, or computer networks of RGS to download or install commercial software, shareware, freeware, promotions, destructive programs (including but not limited to self-replicating codes, viruses, or spam), political or religious material, receipt or distribution of inappropriate or unlawful material as defined above; to participate in or access chat lines, chat groups, or chat sites (unless directly related to the school curriculum and such access has been authorized in advance by the building supervisor or Director of Computer Resources); or to access any site which displays or distributes inappropriate or unlawful material as defined above; or any use which is unauthorized or in violation of School policy, unless given

written permission from the building supervisor or Director of Computer Resources;

- Deliberately performing acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending or forwarding mass mailings or chain letters, spending excessive amounts of time on the internet, playing games, sending or forwarding jokes, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic;
- Copying software for use on their home computers;
- Providing copies of software to any third person;
- Installing software on any computer resources, computers, or computer systems;
- Downloading any software, shareware, freeware, or running executable files from the internet, email, or other online service to any computer resources, computers, or computer systems;
- Modifying, revising, transforming, recasting, or adapting any software;
- Reverse engineering, disassembling, or decompiling any software; and
- Sending, transmitting, or otherwise disseminating proprietary data, trade secrets, or other confidential information of RGS unless expressly authorized by RGS in writing.

## **V. Passwords**

- Responsibility for passwords.* Users are responsible for safe-guarding their passwords for access to the computer systems or computer resources. Individual passwords should not be printed, stored online, or given to others. Users are responsible for all transactions made using their passwords. No User may access the computer system or computer resources with another User's password or account without permission.
- Passwords do not imply privacy.* Use of passwords to gain access to the computer system or to encode particular files or messages does not imply that Users have an expectation of privacy in the material they create or receive on the computer systems or computer resources. The School has global passwords that permit it access to all material stored on its computer system regardless of whether that material has been encoded with a particular User's password.

## **VI. Security**

- Accessing other User's files.* Users may not alter or copy a file belonging to another User without first obtaining permission from the owner of the file. Ability to read, alter, or copy a file belonging to another User does not imply permission to read,

alter, or copy that file. Users may not use the computer system to “snoop” or pry into the affairs of other Users or School operational systems by unnecessarily reviewing their files and email without authority.

- B. *Accessing other computers and networks.* A User’s ability to connect to other computer systems through the RGS computer systems or by a modem does not imply a right to connect to those systems or to make use of those systems unless specifically authorized by the operators of those systems and RGS.
- C. *Computer security.* Each User is responsible for ensuring that use of outside computers and networks, such as the internet, does not compromise the security of RGS computer resources or computer systems. This duty included taking reasonable precautions to prevent intruders from accessing the School’s computer systems via internet connections, or by leaving systems on and logged into the network without authorization, and to prevent the introduction and spread of viruses.

## **VII. Viruses**

*Virus detection.* Viruses can cause substantial damage to computer systems. Each User is responsible for taking reasonable precautions to ensure he or she does not introduce viruses into RGS computer resources or computer systems. To that end, all material received on floppy disk or other magnetic or optical medium and all material downloaded from the internet or from computers or networks that do not belong to RGS must be scanned for viruses and other destructive programs before being placed onto the computer resources or computer systems. All disks transferred from these computers to RGS computer resources or computer systems must be scanned for viruses.

## **VIII. Encryption Software**

- A. *Use of encryption software.* Users may not install or use encryption software on any of RGS’ computers without first obtaining written permission from RGS. Users may not use passwords or encryption passwords that have not been provided to the School’s Technology Coordinator.
- B. *Export restrictions.* The federal government has imposed restrictions on export of programs or files containing encryption technology (such as email programs that permit encryption of messages and electronic commerce software that encodes transactions). Software containing encryption technology is not to be placed on the internet or transmitted in any way outside the United States without the prior written authorization from the School’s Technology Coordinator.

## **IX. Infiltration System**

The RGS computer system has an Internet filtering system that automatically blocks inappropriate websites. However no filter system is 100% effective in blocking all inappropriate content and students must report any unlawful or inappropriate materials as defined above to a teacher or administrator. Despite the filtering system, students are still expected to access the Internet under teacher supervision only.

## **X. Miscellaneous**

- A. *Compliance with applicable laws and licenses.* In their use of computer resources or computer systems, Users must comply with all software licenses; copyrights; and all other state, federal, and international laws governing intellectual property and online activities.
- B. *Other policies applicable.* In their use of computer resources and computer systems, Users must observe and comply with all other policies and guidelines of RGS.
- C. *Computer configuration.* The following items are considered user configurable and may be changed by RGS; screen savor, mouse pointers, additions to the Word Perfect or Word power bar that do not replace the office standard, views in mail, Vision or Word Perfect. Manipulating computer configuration items not in this list may be subject to disciplinary action if not authorized by the School's Technology Coordinator.
- D. *Amendments and revisions.* This policy may be amended or revised from time to time as the need arises. Users shall comply with all amendments and revisions once adopted by RGS.
- E. *No additional rights.* This policy is not intended to, and does not grant, Users any contractual rights.

**XI. Violations and Consequences**

- A. Students who violate this policy shall be subject to revocation of RGS computer resources and computer system access up to and including permanent loss of privileges, and discipline up to and including expulsion.
- B. Disciplinary action may be appealed by parents and/or students in accordance with existing RGS procedures for suspension or revocation of student privileges.
- C. Violations of law by students will be reported to law enforcement officials.

I ACKNOWLEDGE AND UNDERSTAND MY OBLIGATIONS:

Student	Date	Print Full Name
Parent/Guardian	Date	Print Full Name