3321 Acceptable Use of Computer Network(s) Computers and Resources by Teaching Staff Members (M)

The Riverside Township School District supports the use of the Internet, and other information technology, in support of the educational and research goals outlined in our Mission Statement.

All users, including staff, are expected to demonstrate appropriate behavior when accessing network services in the same manner in which they are responsible for behavior in the classroom or school hallways. All general rules for appropriate behavior and communication apply. All staff members should be aware that their work and communication is not confidential when conducted on district electronic technology. This includes email services provided by the district. District personnel, under the direction of school or district administrators, reserve the right to check files and communication logs if necessary.

Related warning: Staff members are strongly discouraged from communicating with students via personal (non-District) e-mail, and are specifically prohibited from doing so via such personal e-mail or social networking media through use of District hardware or the District network.

Communication with parents/guardian

It is expected that teaching staff members may communicate with parents and guardians through e-mail when appropriate and feasible, regarding the general progress of or issues concerning the education of a child, including grades. Specific personal information regarding a student or their family should never be disclosed or discussed via e-mail by a staff member. Nor should any other student be named or discussed in such communication. Should a parent or guardian initiate any such communication, staff members are expected to re-direct the discussion or further contact to other media or to a face-to-face meeting.

Use of District equipment

Any district employee who accepts issue or use of District equipment off-site (e.g. laptop or notebook computers, etc.) accepts full responsibility for any use of that equipment, agrees to be the only user of said equipment, and is expected to maintain the integrity of District equipment and applications. The use of such equipment is limited to the narrow scope of purposes enumerated elsewhere in this policy. Electronic files or data created on District equipment is considered District property. Any inappropriate, illegal or unethical use of District equipment is subject to disciplinary action including, but not limited to, suspension of network privileges, reprimand, suspension, or other District or legal action as might apply.

The following are examples of violations to this acceptable use policy:

Using the network for illegal purposes.

Illegal activities shall be defined as a violation of local, state, and/or federal laws. Do not violate copyright laws. Loading of software or attempting to copy software to or from the district's computers is prohibited by this policy and federal law. If you need to have

software installed, please contact the district Technology Specialist. Any violation of Fair Use Guidelines is prohibited. Materials accessed through the Internet must be properly cited when referenced in a user research assignment. The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to misuse of the district's information network.

Using the network for inappropriate purposes

Inappropriate use shall be defined as a violation of intended use of the network, and/or purpose and goal. This includes but is not limited to: accessing sites that contain pornography, vulgar or obscene language, racist, sexist or ethnic remarks, or any other uses deemed objectionable in a public school environment. Any user accessing the Internet must have specific research objectives or communications that are based on classroom assignments, authorized professional development activities, or the operation of the district and its departments. Investigation by school or district administrators in disciplinary matters shall constitute authorized use. When using another organization's network or computing resources, you must comply with the rules appropriate to that network.

Vandalism

Any malicious attempt to harm or to destroy equipment or data on the district's or any outside agency or network to which the district is connected is a violation of this policy. This includes, but is not limited to damaging equipment, altering files, uploading, downloading, or creation of computer viruses, worms, or other damaging programs.

Gaining access to unauthorized areas of the network.

Any attempt to gain unauthorized access to others' files, or vandalizing data of another user is prohibited. Any security problem should be promptly reported to the system administrator. Security problems should never be demonstrated to others.

Disruption of network traffic.

Do not use the network in any way that would disrupt the use of the network. Users are specifically prohibited from utilizing live radio broadcasts or music sites via the internet, playing games, communicating with chat rooms, watching videos, or downloading large files unless these activities are directly related to educational activities for a lesson, authorized professional development activities, or aforementioned disciplinary investigation.

Using the district's resources for commercial gain.

The network and Internet access is provided for users to conduct educational research and to communicate with others. Any use of the resources for financial gain or political activity is inconsistent with the purpose of the information system.

Forging electronic mail messages, or using an account owned by another user.

An employee should only use the login name that has been assigned to him or her by the district. The use of another person's account, or allowing another to use one's account, is also prohibited. Employees are expected to protect the integrity of their passwords, and to have such passwords changed as soon as possible if they believe they have been

compromised. Employees are responsible for protecting their account on the district's information system and are responsible for its use at all times.

Posting anonymous messages.
Any messages posted on the network or the Internet must have the sender's name attached. This will happen by default without user intervention.

Possession of materials in violation of these rules.
You may not possess any data or software, which might be considered a violation of these rules in paper, CD, DVD, magnetic (disk), or any other form.

Not abiding by general rules of etiquette.
You must abide by general rules of etiquette. Not abiding can come in many forms and includes but is not limited to sending abusive messages, using vulgar or obscene language, racial, sexist, or ethnic slurs. Please remember that using all uppercase characters is considered shouting when using electronic communication.

Divulging personal information.
Personal information about yourself or others should never be divulged. Personal information such as an address, telephone number, or social security number should not be divulged to anyone on the Internet. District contact information should not be divulged to others outside of the school district.

Wastefully using finite resources.
Resources should not be used needlessly. These can include, but are not limited to: using resources for frivolous purposes when others have need of them for educational purposes, the printing of large documents when a printing of selected pages would suffice, storing of files on network drives that are not consistent with the adopted curriculum and educational objectives of the district. The printers are to be used only for original documents and are not a substitute for copying.

Modifying system configurations or settings.
Users are not allowed to change any settings or configurations on any computer. This includes, but is not limited to changing wallpapers, screen savers, printers, deleting needed files, or any other settings. Users are specifically prohibited from installing any programs onto local or network drives or disks. This includes freeware, shareware, or commercial downloads from the web, as well as disk or CD based programs. Any executable files (programs) that were not part of the original configuration and are found on a local or network drive will be considered a direct violation of this policy. File sharing software and services such as but not limited to: Kazaa, Morpheus, LimeWire and WinMX are prohibited.

Adding or modifying hardware
Users are not allowed to bring in any computers, monitors, printers or any other hardware without permission from the Technology Specialist and the appropriate administrator. It is especially critical that users do not connect any non-district computer, laptop, or wireless access points to any port on the network. Such actions present a significant security risk to the entire network and are specifically prohibited. The Board of Education

will not be held responsible for any personal technology equipment used in school facilities or in any school-related work.

The following additional policies apply to staff members to help protect our students and to help shield the staff member and district from potential liability:

The Riverside Township School District encourages staff to create and post web pages to help inform students and the community about the school, policies, and activities. The following explains the responsibilities and procedures to be followed when having the students use the Internet or when posting school and/or classroom web pages.

The district has a student Acceptable Use Policy that signed parental permission be provided to be able to:

1. Allow a child to access the Internet as part of class activities.

2. Post a child's work so that it may be electronically displayed and published on the District web site. This publishing would display a child's work and their name, class and grade would be associated with the work, but no other personal information would be provided.

3. Post anonymous photographs (with no name association) of a child or group pictures including a child on the district's web site.
   Examples of this could include a picture of a teacher's class on a field trip, a picture of activities in a science class, or pictures of the field hockey team. Only general information regarding the picture would be given, but no personal information about those in the picture would be provided.

Int

All schools will collect these signed permission forms and the permissions will be entered into each building's student database. The following guidelines should be followed:

- When posting information to a class, building or district web site, under no circumstances should a student's address or phone number be included. If replies to a student's work are appropriate, the sponsoring teacher's email address should be displayed, not the student's.

- Students should not be required to give out personal information on any website to which a staff member is directly associated. If a staff member chooses to develop a website that staff member is responsible for the content of that site.

- If a student has not been given parental permission to access the Internet, other appropriate activities should be provided.

Consequences for Violations

Violations will result in loss of Internet access and/or district or other computer use. Other disciplinary actions may be determined at the building or district level in line with existing practices regarding inappropriate student or employee behavior. When applicable, law enforcement agencies may be notified.

Legal References

N.J.S.A. 2C:20-23 et seq. Computer Related Crimes Act
N.J.S.A. 2C:21 Anti-Privacy Act
N.J.S.A. 2C:20-2 Consolidation Act
N.J.S.A. 18A:73-44 Library Privacy Act

-Computer fraud, see 18 U.S.C.A. 1030
-Copyright, scope and subject matter, see 17 U.S.C.A. 101 et seq.
- Federal computer systems, standard and technology, see 15 U.S.C.A. 278g-3
- High performance computing and application, see 15 U.S.C.A. 5501 et seq.
- Limitations on exclusive rights for computer programs, see 17 U.S.C.A. 117
- National high-performance computer program, see 15 U.S.C.A. 5511
- Notice of copyright, see 17 U.S.C.A. 401
- Protection of semiconductor chip products, see 17 U.S.C.A. 901 et seq.
- Recording of documents pertaining to computer shareware and donation of public domain computer software, see 37 CFR 201.26, 17 U.S.C.A. foll. 702
- Scheme or artifice to defraud, definition of, see 18 U.S.C.A. 1346
- Unauthorized publication or use of communications, see 47 U.S.C.A. 605
- Unlawful access to stored communications, see 18 U.S.C.A. 2701
- Visual arts registry, see 37 CFR 201.25, 17 U.S.C.A. foll. 702
- Warning of copyright for software lending by non-profit libraries, see 37 CFR 201.24, 17 U.S.C.A. foll. 702
- Wire and electronic communications interception, see 18 U.S.C.A. 2510 et seq.
- Wire fraud, see 18 U.S.C.A. 1343

Adopted: 12 May 2010