

*Administrative Rule*

**ELECTRONIC COMMUNICATIONS AND DATA MANAGEMENT  
(ADMINISTRATIVE PROCEDURES FOR ACCEPTABLE USE GUIDELINES)**

Code **IJND-R** Issued \_\_1/2009\_\_

---

This administrative rule governs the use of the District's computers, network, Internet and electronic research and communication resources and is intended to protect the integrity of District operations and instructional programs, as well as to outline the rights and responsibilities of District employees and students. These rules shall be in effect at all times and places whether on or off of District property.

**Scope**

This administrative rule applies to the following persons/entities:

- All District employees including regular, part-time, temporary and contract employees
- All students enrolled in District schools
- All other authorized users of any of the District's technology resources, regardless of District affiliation or reason for usage
- All District owned or operated technology resources or systems which are subscribed to and/or paid for by the District

**Confidential Information**

The District's research, information and communication resource systems have security measures in place; however, such measures do not guarantee total security. As a result, information generally considered to be personal or confidential should not be sent via the District's communication resources except through means deployed for that purpose or approved for that purpose by the Information Services Division. The District cannot assume responsibility for lost or stolen information sent or received via the District's communication resources.

**General Computer Usage**

The following actions are prohibited:

- Knowingly loading or creating viruses
- Loading or attempting to load software or files onto a school computer without the permission of the school's Instructional Technology Specialist
- Loading or attempting to load software or files onto the District network without the permission of the Information Technology Department
- Accessing or modifying data without authorization
- Modifying passwords without authorization

## **PAGE 2 – IJND-R – ELECTRONIC COMMUNICATIONS AND DATA MANAGEMENT (ADMINISTRATIVE PROCEDURES FOR ACCEPTABLE USE GUIDELINES)**

- Computer vandalism, defined as any malicious or unauthorized attempt to harm or destroy equipment or data, files, or other electronic information not belonging specifically to the user
- Destruction of electronic records once the potential for litigation has been identified

### **Network and Internet Usage**

Access to the district network and Internet is made available to authorized users for educational and District operational purposes. All authorized users will receive instruction on proper use of the District's network and Internet system.

The District will not be liable for the users' inappropriate use of the District's electronic communication resources or violations of copyright restrictions, users' mistakes or negligence, or costs incurred by users. The District will not be responsible for ensuring the accuracy or usability of any information found on the Internet.

The District prohibits the use of its network and the Internet to intentionally access, view, download, store, transmit, or receive any information that contains material which is in violation of any District policy or administrative rule, or any local, state and/or federal laws or regulations. Prohibited material includes, but is not limited to:

- Obscenity or pornography
- Threats
- Material that is intended, or could reasonably be perceived, to be harassing or discriminatory
- Material that is copyrighted or protected by trade secret
- Material used to further any commercial business, product advertising, virus transmission or political activity
- Material that is potentially disruptive of the learning environment

The District reserves the right to monitor and/or review all uses of the District network and the Internet, and users should not have any expectation of privacy in any information accessed, viewed, downloaded, stored, transmitted, or received.

### **Electronic Mail (Email) Usage**

The District's email system is made available to authorized users for educational and District operational purposes. All authorized users will receive instruction on proper use of the District email system.

The District prohibits the use of its email system for unprofessional and/or inappropriate purposes, to include, but not be limited to:

- Creating, transmitting or receiving emails containing any language or depictions that could reasonably be perceived by others as being offensive, threatening, obscene, sexual, racist, or discriminatory

**PAGE 3 – IJND-R – ELECTRONIC COMMUNICATIONS AND DATA MANAGEMENT  
(ADMINISTRATIVE PROCEDURES FOR ACCEPTABLE USE GUIDELINES)**

- Any use that violates local, state and/or federal laws or regulations
- Setting up or operating a commercial business

All electronic messages created, transmitted or received via the District's email system, including those created, transmitted or received for personal use, are the property of the District. The District reserves the right to archive, monitor and/or review all use of its email system and users should not have any expectation of privacy in any electronic message created, transmitted or received on the District's email system.

**Handheld Communication Device Usage**

District-issued cell phones or other handheld communication devices are to be used only by the employee to whom the phone or communication device was issued and are to be used only for matters directly related to the employee's job responsibilities. The District reserves the right to monitor and/or review all use of District-issued phones and communication devices and users should not have any expectation of privacy in any use of a District-issued phone or communication device.

**Personal Use of District Research, Information and Communication Resources**

Limited personal use of District computers, the District network and the Internet and electronic research and communication resources is permitted to the extent that such use does not disrupt or interfere with the operation of the District and its instructional programs. Excessive personal use that may or does so disrupt or interfere is prohibited.

**Third Party Access to Systems and/or Data**

Within limited circumstances, Richland School District Two sub-contracts specific work to be performed on behalf of the district in areas including, but not limited to, software development, system support, hardware acquisition and provisioning, and training. As part of these agreements, specific authority is granted to the sub-contracted third party to access the district's network and data, including student information and financial information. These agreements and authorities of access to systems, networks or data are temporary in duration and bound by non-disclosure principles, confidentiality and time frames established within the agreement between the district and any third party. All local, state and federal statutes, laws or regulations regarding confidentiality of student information or financial information apply.

Sub-contracted work being performed on behalf of the district is limited to the specified parameters within the agreement. Upon completion of the agreed upon work, access to district systems or data is to be considered terminated. This termination of access shall be accomplished either by manual action taken by Richland Two Information Services, or considered as the default access status of the third party following the completion of agreed upon work or tasks.

At no time shall access to systems or data be continued beyond the completion of work, or duration of specified time. Any physical or virtual access, either locally or remotely, to networks, systems or data must be approved by Richland School District Two Information Services or the

**PAGE 4 – IJND-R – ELECTRONIC COMMUNICATIONS AND DATA MANAGEMENT  
(ADMINISTRATIVE PROCEDURES FOR ACCEPTABLE USE GUIDELINES)**

district superintendent. No other district entity holds the authority to grant access to any networks, systems or data. In circumstances where access is granted, the specific access is valid only for the duration of specifically agreed upon work and/or time frames. At the completion of agreed upon work, access is considered terminated. Once access is considered terminated, new authority of access must be granted by Richland School District Two Information Services or the district superintendent prior to any new work, continuance of work, or attempted access. Continuance of access authority is never automatic or to be assumed by any third party.

**Violations**

All authorized users of District research and communication resources are expected to report any use that is believed to be unauthorized, excessive or otherwise in violation of this administrative rule. District employees who witness, experience, or otherwise learn about a suspected violation should report the matter to their immediate supervisor. Students who witness, experience or otherwise learn about a suspected violation should report the matter to a teacher or school administrator. Other authorized users who witness, experience, or otherwise learn about a suspected violation should report the matter to a District administrator.

An employee's personal use of non-District issued electronic communications resources outside of working hours will be the concern of and warrant the attention of the Board if it impairs the employee's ability to effectively perform his or her job responsibilities or as it violates local, State, or federal law, or contractual agreements. (See policy GBEB regarding use of non-District issued electronic resources.)

All suspected violations will be investigated thoroughly. If it is determined that a violation of this administrative rule has occurred, the following disciplinary and/or corrective actions may be taken:

- Review of and possible changes to the level of supervision and the circumstances under which use is allowed
- Limitation, suspension and/or termination of the violator's use privileges
- For student violators, disciplinary measures consistent with the District's student discipline code, up to and including expulsion
- For employee violators, disciplinary measures determined to be appropriate based on the seriousness of the violation, up to and including termination
- Report to law enforcement when the violation is believed to constitute a violation of a state or federal law or regulation

Adopted 10/96; Revised \_01/2009