

# Technology

Proper use of technology can enhance teaching and learning. For our students to be successful in an ever changing and dynamic world they must be:

- Creators
- Communicators
- Collaborators
- Critical Thinkers

Technology is a valuable tool to help our students meet these world class skills. However, it must be used properly to optimize its potential and avoid unintended consequences.

School Board policy IJNDB [Use of Technology Resources](#), provides specific guidance for the proper use of technology. It is important that you become familiar with this policy and fully comply with its tenets. The policy is provided in its entirety on pages 57-62 of the Board Policy section of this Handbook.

## **Technology – Supplemental Guidelines**

The guidelines below expand on or clarify Policy IJNDB – Use of Technology.

While Policy IJNDB provides an excellent framework and overarching guide for the use of technology, there are some additional guidelines and procedures that must be followed by all District Five employees.

These guidelines are provided so

the user is aware of the responsibilities he/she must assume. In general, these guidelines require efficient, ethical, and legal utilization of the technology resources.

### **Privileges**

The use of the internet is a privilege, not a right. Violations of these guidelines may result in the loss of internet access privileges and appropriate discipline and/or legal procedures consistent with existing policies and procedures of District Five of Lexington and Richland Counties.

### **Network Etiquette**

The user is expected to abide by the generally accepted rules of network etiquette. Etiquette rules include, but are not limited to, the following:

The user must be polite. Do not use abusive or harsh language in messages to others.

- Appropriate language must be used. No swearing, use of vulgarities or any other inappropriate language is allowed. Illegal activities are strictly forbidden.
- The user should properly identify himself/herself including their position/title in every email correspondence.
- The user should not reveal his/her personal address or phone number or those of others.

### **Security**

Security on any computer system is a high priority, especially when the system involves many users. If the user feels he/she can identify a technology security problem he/she must notify the

District Director of Technology and his/her school principal.

- The user must not attempt to log on to the internet as a system administrator.
- Users must not share their password (or other person's passwords) with another person or leave an open file or session unattended or unsupervised.
- Account owners are ultimately responsible for all activity under their accounts.
- Users shall not seek information on, or obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system or attempt to gain unauthorized access to the system.
- Communication may not be encrypted so as to avoid security review.
- Users must change passwords regularly and avoid easily guessed passwords on any district account, including school accounts used for accessing websites or other online resources.
- For security and administrative purposes, the District reserves the right for authorized personnel to review system use and file content including, without limitation, the content of any electronic mail.
- Users must not install or attempt to install software, programs or other devices that require admin credentials on district devices.

Any user identified as a security risk or having a history of problems with other computer systems may be denied access to internet and/or district systems.

### ***Vandalism***

Vandalism may result in the loss of internet access privileges and appropriate discipline and/or legal procedures consistent with existing policies and procedures of District Five of Lexington and Richland Counties. This includes physical damage to any technology device as well as uploading or creation of computer viruses or other actions to slow, harm or disable a specific device, the District network or any other network.

### ***Copyright***

The unauthorized installation, use, storage or distribution of copyrighted software or materials on District computers is prohibited.

### ***Cell Phone Usage***

The use of cell phones in classrooms is prohibited except during a teacher or teacher assistant's planning or break time. Cell phones should be left off while teachers or teacher assistants are engaged in instruction or when students are in the room, unless prior permission has been obtained from the principal due to an emergency situation.

### ***Social Media***

- Employees should assume nothing is confidential on the internet or social media.
- All staff must recognize that they are being continuously observed by students, other employees, parents, and community members, and that their actions and demeanor may impair their effectiveness as an

employee.

- The personal life of an employee, including the employee's personal use of non-District issued electronic equipment outside of working hours (such as through social networking sites and personal portrayal on the internet), will be the concern of and warrant the attention of the Board if it impairs the employee's ability to effectively perform his/her job responsibilities or if it violates local, State, or federal law or contractual agreements.

Unprofessional content or conduct on social media sites may subject the employee to disciplinary actions consistent with State law, federal law, and/or Board policy.

- All employees shall maintain a professional relationship with students at all times, both inside and outside of school. Social media must not be used to create relationships with students outside the professional relationship required to perform your job.
- No employee may engage in inappropriate conduct of a sexual nature with a student at any time. This includes electronically through such means as a telephone, cell phone, computer, personal data assistant, or other telecommunication device, including text messaging and social networking.
- Employees should not include any District student in social networking activities or provide students with access to their social networking activities through the internet. Employees should not "friend" District students on the internet or through social networking sites, either by allowing students access to the

employee's site, or the employee accessing the student's site.

- Employees should not share or post on the internet or on personal social networking sites student information, including student photographs, student work, or student activities without the prior approval of the school administration and the student's parent. This prohibition does not apply to sharing student's work or photographs through District approved means that are related to instruction.
- Employees must not conduct non-work related business during work hours. Employees should not access social networking sites, conduct internet searches that are not related to District business, or engage in the inappropriate use of other electronic forms of communication during work hours.

### ***General Use***

- Employees and students must use the District network while on school property. Use of mobile "hot spots" or other outside networks is prohibited. (policy JICJ)
- The Executive Director of Operations or designee must approve use of the system for charitable purposes in advance.
- The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures. (policy KHE)
- Diligent effort must be made to conserve system resources. For example, users should frequently delete E-mail and unused files. The District reserves the right to remove a user account on the system for any reason.