

The purpose of the Acceptable Use Policy is to inform parents, guardians, and students of the rules governing the use of district and personal technology resources while on or near school property, in school vehicles, and at school-sponsored activities, as well as the use of district technology resources via off-campus remote access. In addition, your student's image may be used on promotional materials as well as on the school-sponsored website.

#### INTRODUCTION:

Rossville Consolidated School District is pleased to offer students access to district computers, communication systems (i.e. student e-mail accounts, web sites, blogs, wilds, podcasts, and other emerging technologies), the Internet, and an array of technology resources to promote educational excellence. Each student is responsible for his/her use of technology, whether personal or district-provided. While using district and personal technology resources on or near school property, in school vehicles, and at school-sponsored activities, as well as using district technology resources via off-campus remote access, each student must act in an appropriate manner consistent with school, district, and legal guidelines. It is the joint responsibility of school personnel and the parent or guardian of each student to educate the student about his/her responsibilities and to establish expectations when using technology.

#### USING THE INTERNET AND COMMUNICATION SYSTEMS:

District technology resources are provided to students to conduct research, complete assignments, and communicate with others in furtherance of their education. Access is a privilege, not a right: as such, general rules of school behavior apply. Access to these services is given to students who agree to act in a considerate and responsible manner. Just as students are responsible for good behavior in a classroom or a school hallway, they must also be responsible when using school computer networks or personal technologies. Students must comply with corporation standards and honor this agreement to be permitted to use technology.

All digital storage is district property, and as such, network administrators will review files and communications to maintain system integrity and ensure that students are using technology responsibly. Students should not expect that files stored on district servers will be private. It is the responsibility of the student to back up his/her files whenever a new file is created or an old file has been edited and changed. Files may be backed up by storing them on the server, in the cloud, a personal storage device (such as a flash drive), or burning them to a CD.

The educational value of technology integration in curriculum is substantial. Access to the Internet will enable students to use extensive online libraries and databases. Families should be warned that some material accessible via the Internet might contain items that are illegal, defamatory, inaccurate, profane, sexually oriented or potentially offensive to some people. While the intent is to make internet access available to further educational goals and objectives, students may find ways to access these other materials as well such as on personal cell phones or devices. Rossville Consolidated School District does not condone or permit the use of this material and uses content filtering software to protect students to the fullest extent possible. If a website is blocked by the school filter, students should not try or hack to "get around" the filter. Parents and guardians must be aware that content filtering tools are not completely fail-safe and while at school, direct supervision by school personnel of each student using a computer is desired, but not always possible. Students are expected to use technology resources in a manner consistent with the rules below and will be held responsible for their intentional misuse.

Any District computer used by students shall have Internet filtering software in place either on the computer itself, or on the server through which the computer accesses the Internet.

District staff shall not allow students to use any computer in the District with Internet capability that does not have Internet filtering software. This includes any computer, laptop or desktop, in the District's Libraries or media centers, classrooms, laboratories, or offices where students are, for any reason, allowed to use a computer, or any other such device, with Internet access. Staff members violating these rules are subject to disciplinary action up to and including discharge.

Rossville Consolidated School District believes that the benefits of student access to the Internet in the form of information resources and opportunities for collaboration exceed any disadvantages. Ultimately, parents and/guardians are responsible for setting and conveying the standard that their children should follow when using technology. If a student accidentally accesses inappropriate materials, they should back out of the information at once and notify the supervising adult.

#### PROPER AND ACCEPTABLE USE OF ALL TECHNOLOGY RESOURCES:

All district technology resources, including but not limited to district computers, communication systems, and the Internet, must be used in support of education and academic research and must be used in a manner consistent with the educational mission and objectives of Rossville Consolidated School District.

Activities that are permitted and encouraged include:

- School work
- Original creation and presentation of academic work
- Research on topics being studied in school
- Research for opportunities outside of school related to community service, employment,

or further education

SECTION 621 - STUDENT ACCEPTABLE USE POLICY (Continued)

3 of 4

Activities that are not permitted nor encouraged include:

- Plagiarism or representing the work of others as one's own
- Using obscene language, harassing, insulting, ostracizing, or intimidating others
- Representing Copyright, Registered, and/or Trademark materials as one's own work
- Searching, viewing, communicating, publishing, downloading, storing, or retrieving materials that are not related to school work, community service, employment, or further education (thus, searching inappropriate materials is not permitted)
- Damaging or modifying computers, software, or networks with permanent materials
- Intentional or neglectful transmission of viruses or other destructive computer files; hacking into district or external computers, intentionally bypassing district filters
- Use of USB, boatable COs, or other devices to alter the function of a computer or a network
- Subscription to any online services or ordering of any goods or services
- Online sharing of any student's or staff member's name, home address, phone number, or other personal information
- Non-educational uses such as gambling, junk mail, chain mail, jokes, raffles
- Participating in online chat rooms or using instant messaging, unless specifically assigned by a teacher
- Use of district resources for commercial purposes, personal financial gain, or fraud
- Any activity that violates a school rule or a local, state, or federal law

Students are expected to report harassment, threats, hate-speech, and inappropriate content to a teacher or administrator. If a student has any questions about whether a specific activity is permitted, he or she should ask a teacher or administrator.

**PRIVACY AND SECURITY:**

Students must use corporation technologies responsibly and in a secure manner. They must not share their logins, passwords, or access with others.

**VANDALISM:**

Any intentional act by a student that damages district technology hardware, software, operating systems, or data will be considered vandalism and will be subject to school rules and disciplinary procedures. Any intentional act that requires a person's time to repair, replace, or perform corrective work on district technologies or data is also considered vandalism. Students should report lost or broken items to their teacher or administrator immediately.

**CONSEQUENCES OF MISUSE:**

Misuse of personal or district technology resources while on or near school property, in school vehicles, and at school-sponsored activities, as well as the use of district technology resources via off-campus remote access may result in disciplinary action up to and including expulsion. This document shall be used in conjunction with the Rossville Consolidated School District Board of Education policies and our school handbooks. In addition, the student's use of district technologies may be suspended or restricted. A school may temporarily hold (pending parental or same-day pick up) personal technology resources that are used inappropriately. Intentional, unauthorized access and/or damage to networks, servers, user accounts, passwords, or other district resources may be punishable under local, state, or federal law.

**RELIABILITY AND LIMITATION OF LIABILITY:**

Rossville Consolidated School District makes no warranties of any kind, expressed or implied, for the technology resources it provides to students. Rossville Consolidated School District will not be responsible for any damages suffered by the student, including those arising from non-deliveries, misdeliveries, service interruptions, unauthorized use, loss of data, and exposure to potentially harmful or inappropriate material or people. Use of any information obtained via the Internet or communications technologies is at the student's own risk. Rossville Consolidated School District specifically denies any responsibility for the accuracy or quality of information obtained through the Internet. The student and his/her parent/guardian will indemnify and hold Rossville Consolidated School District harmless from any losses sustained as the result of misuse of the district's technology resources by the student.

**NOTICE:** This policy and all its provisions are subordinate to local, state, and federal statutes.

*DATE ADOPTED:* June 5, 2001

*DATE REVISED:* March 14, 2002  
May 13, 2003  
February 17, 2004  
June 1, 2010  
June 3, 2014

*DATE REVIEWED:* March 14, 2006  
December 16, 2014

## RATIONALE

Rossville Schools have an obligation to maintain a safe physical and emotional environment, and a responsibility to consult with the community.

The Rossville School Board places a high priority on providing the school with Internet access and Information Communication Technologies (ICT) devices / equipment which will benefit student learning outcomes, and the effective operation of the school.

The Rossville School Board recognizes that the presence in the learning environment of these technologies (some provided partly or wholly by the school and some privately owned by staff, students and other members of the school community), can also facilitate anti-social, inappropriate, and even illegal, material and activities. The school has the dual responsibility to maximize the benefits of these technologies, while at the same time to minimize and manage the risks.

The Rossville School Board thus acknowledges the need to have in place rigorous and effective school cybersafety practices which are directed and guided by this cybersafety policy.

## POLICY

Rossville Schools will develop and maintain rigorous and effective cybersafety practices which aim to maximize the benefits of the Internet and ICT devices/equipment to student learning and to the effective operation of the school, while minimizing and managing risks.

These cybersafety practices will aim to not only maintain a cybersafe school environment, but also aim to address the need of students and other members of the school community to receive education about the safe and responsible use of present and developing information and communication technologies. Rossville Schools will provide for the education of minors about appropriate online behavior, including but not limited to; interacting with other individuals on social networking websites and in chat rooms, and cyber bullying awareness and response.

## POLICY GUIDELINES

Associated issues the school will address include: the review of the school's annual and strategic plan, the deployment of staff, professional development and training, implications for the design and delivery of the curriculum, the need for relevant education about cybersafety for the school community, disciplinary responses appropriate to breaches of cybersafety, the availability of appropriate support, and potential employment issues.

To develop a cybersafe school environment, the board will delegate to the principal the responsibility to achieve this goal by developing and implementing the appropriate management procedures, practices, electronic systems, and educational programs.

A process for reporting back to the board by the principal will be agreed upon and established. Frequency and content of reporting will be included.

#### Guidelines for Rossville Schools Cybersafety Practices

1. The school's cybersafety practices are to be based on information contained in the latest version of the approved curriculum.
2. No individual may use the school Internet facilities and school-owned/leased ICT devices/equipment in any circumstances unless the appropriate use agreement has been signed and returned to the school. Use agreements also apply to the use of privately-owned/leased ICT devices/equipment on the school site, or at/for any school-related activity, regardless of its location. This includes off-site access to the school network from school or privately-owned/leased equipment.
3. Rossville Schools use agreements will cover all board employees, all students (including adult and community), and any other individuals authorized to make use of the school Internet facilities and ICT devices/equipment, such as staff, teachers, student teachers, internal/external tutors and providers, contractors, and other special visitors to the school.
4. The use agreements are also an educative tool and should be used as a resource for the professional development of staff.
5. Use of the Internet and the ICT devices/equipment by staff, students and other approved users at Rossville Schools is to be limited to educational, professional development, and personal usage appropriate in the school environment, as defined in individual use agreements.
6. Signed use agreements will be filed in a secure place, and an appropriate system devised which facilitates confirmation that particular individuals are authorized to make use of the Internet and ICT devices/equipment.
7. The school has the right to monitor, access and review all use. This includes personal emails sent and received on the schools computer/s and/or network facilities at all times.
8. The school has the right to audit at anytime any material on equipment that is owned or leased by the school. The school may also request permission to audit privately owned ICT devices/equipment used on the school site or at any school related activity.

9. The safety of children is of paramount concern. Any apparent breach of cybersafety will be taken seriously. If illegal material or activities are suspected, the matter shall be reported to the appropriate law enforcement agency.

*DATE ADOPTED:* June 1, 2010

*DATE REVISED:* May 15, 2012  
December 16, 2014