Rush County Schools
Responsible Use of Technology Policy

Educating Students with Technology Today for their Digital Success Tomorrow

Approved by the Rush County Schools Board of Trustees
5/23/16

Definitions

"Confidential information" means information that is declared or permitted to be treated as confidential by state and/or federal law and/or Board Policy on access to public records.

"Personally Identifiable Information" includes, but is not limited to: a. The student's name; b. The name of the student's parent or other family member; c. The address of the student or student's family; d. A personal identifier, such as the student's social security number or student number; e. A list of personal characteristics that would make the student's identity easily traceable; or f. Other information that would make the student's identity easily traceable. (FERPA -- Federal Education Rights and Privacy Act)

"Communications System" defines all electronic mediums of communication, including telephone systems, technology networks, voicemail systems, and communication platforms such as chat or email.

"Technology" defines all electronic devices, associated software, and the systems that support those devices.

"Network" refers to the connections between technology devices and supporting systems of an entity, such as a school district.

"Internet" refers to the broader network of systems and connections throughout the world that relay information for connected technology.

"Personal device" includes cell phones, smart phones, laptops, slates, handhelds, e-readers, tablets, or any other technology devices that are not the property of the school[1].

"School provided device" includes cell phones, smart phones, laptops, slates, handhelds, e-readers, tablets, Chromebooks, or any other technology device that is the property of the school.

"Technology Director" means the School Board of Directors (Board) employee designated by the Superintendent to maintain and/or operate the school's technology.

"Technology Coordinator" means the Board employee(s) designated by the Superintendent to support the Technology Director's efforts to maintain and/or operate the school's technology.

"User" means a Board employee, student, volunteer, contractor, or other person authorized to use ~~Board~~ school technology.

"Social media" means media that allows people to create, share or exchange information, career interests, ideas, and pictures/videos in virtual communities, i.e. Facebook, Twitter, LinkedIn.

[1] In this policy, "school", "schools", "school district", and "Corporation" are used to represent the property of the "Board" and "Rush County Schools Board of Directors"

Responsible Use At School

1. Purpose

1.1. The Rush County School District (Corporation) encourages its users to utilize technology, the network, and the Internet in order to promote educational excellence in our schools by providing them with the opportunity to develop the resource sharing, innovation, and communication skills and toolset that are essential to both life and work.

1.2. The Corporation's network has a limited educational purpose and has not been established as a public access service or a public forum.

1.3. Online content (such as websites) posted to the public must serve the purpose to educate, inform, and communicate.

1.3.1. Content provided in the websites should be usable by students and teachers to support the curriculum, school objectives and school strategic plan.

1.3.2. Content may inform the community about public school information, such as events, curriculum, class projects, activities, policies, and procedures.

1.3.3. Content may be used to communicate with the community in a constructive fashion.

1.4. The Corporation has the right to place restrictions on its use to assure that use of the Corporation's network is in accord with its limited educational purpose.

1.5. Use of the Corporation's technology, network, and Internet access will be governed by this policy, the related administrative guidelines, the Student and Staff Codes of Conduct, 1 to 1 pledges, and accompanying procedures.

2. Scope

2.1. This policy applies to all technology, devices, network, and Internet access at school, including personal devices that are on the buildings and grounds of Rush County Schools.

2.2. (This policy does not address the Lending of Corporation-Owned Equipment found in Board Owned Personal Communication Devices and Staff Use of Personal Communication Devices, see Policy 7530).

3. Requirements

3.1. Pursuant to Federal law, students shall receive education about the following:

3.1.1. Safety and security while using e-mail, chat rooms, social media, and other forms of direct electronic communications;

3.1.2. The dangers inherent with the online disclosure of personally identifiable information;

3.1.3. The consequences of unauthorized access (e.g., "hacking"), cyberbullying and other unlawful or inappropriate activities by students online; and

3.1.4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.

3.2. Staff members shall provide instruction to their students regarding the appropriate use of technology and online safety and security as specified above.

3.3. Furthermore, staff members will monitor the online activities of students while in school.

3.4. The Corporation has implemented the use of technology protection measures which are specific technologies that will protect against (e.g. filter or block) access to visual displays/depictions that are obscene, pornographic, and other materials harmful to minors, as defined by the Children's Internet Protection Act.

3.5. Protection of protected student information and personally identifiable information must be maintained regardless of where information is stored (such as the "cloud") as required by the FERPA Act.

4. Responsibilities

4.1. Users are responsible for good behavior on the Corporation's technology, Corporation's network and the Internet just as they are in classrooms, school hallways, and other school premises and school sponsored events.

4.2. Communications on the Internet are often public in nature. General school rules for behavior and communication apply.

4.3. The Corporation does not sanction any use of the Internet that is not authorized by or conducted strictly in compliance with this policy and its accompanying guidelines.

4.4. Students and other users of school technology are to practice their digital citizenship skills at all times. Training will be provided to students and staff on essential digital citizenship skills.

4.5. All users are responsible for compliance with all trademark, patent, copyright laws, and applicable license and contractual agreements.

4.6. Users are responsible for protecting their personal information online, including user account names and passwords. Everybody has a responsibility to keep their accounts safe and not share them with others.

4.7. Users are responsible for using email responsibly and for its educational and school business purposes.

4.8. Use of a camera and/or microphone must be done so in appropriate situations and for educational use only.

4.9. Many online services allow users to collaborate on work (such as Google Apps for Education). Use of these services must be for educational use.

4.9.1. Examples of responsible use may include working together on a group project or providing constructive feedback for others.

4.9.2. Examples of irresponsible use may include inappropriate chatting with friends inside a workspace, playing inside a document instead of performing class work, or sharing for the purpose of cheating.

4.10. The ability to share information online with sharing functionality must be used responsibly and with great care. Use the most restrictive sharing that satisfies the the purpose of sharing the information with the appropriate members. Do not share globally or publicly unless it is safe to do with the information in question.

4.11. If a website that contains inappropriate material is inadvertently accessed, it is the student's responsibility to report the problem to the teacher, and it is the staff member's responsibility to report the problem to an administrator.

4.12. Students shall not access social media for personal use from the Corporation's network or school provided devices, but shall be permitted to access social media for educational use in accordance with their teacher's approved plan for such use. Administrative and technical approval is required before granted access to specific social media for educational use.

4.13. Federal and State confidentiality laws forbid schools and their employees from using or disclosing student education records without parent consent (see Policy 8330). Education records include a wide variety of information.

4.14. Posting personally identifiable information about students is not permitted. Staff members who violate State and Federal confidentiality laws or privacy laws related to the disclosure of confidential student or employee information may be disciplined.

4.15. An employee's personal or private use of social media, such as Facebook, Twitter, and blogs, may have unintended consequences. While the Board respects its employees' First Amendment rights, those rights do not include permission to post inflammatory comments that could compromise the Corporation's mission, undermine staff relationships, or cause a substantial disruption to the school environment. This warning includes staff members' online conduct that occurs off school property including from the employee's private computer. Postings to social media should be done in a manner sensitive to the staff member's professional responsibilities.

4.16. Furthermore, connecting with students on social media may have unintended consequences. Therefore, an employee's personal or private use of social media will not be used to establish connections (such as "friending") of any enrolled student of Rush County Schools, regardless of building or grade level, except where the relationship is that of a student family member.

4.17. Online content that is visible to the public (such as websites) that users create is authorized under the following conditions.

4.17.1. Content must reflect the professional image of the schools.

4.17.2. Content must not include protected and personally identifiable information that is in violation of this policy.

4.17.3. When the content includes a photograph or information relating to a student and/or staff, including Corporation-issued email accounts, the Corporation will abide by the provisions of Policy 8330 - Student Records.

4.17.4. Links to other content must also reflect the professional image of the schools.

4.17.5. Links to news and media outlets, and other sites that include commercial vendors contracted with the school, must contain age-appropriate advertisements (see Policy 9700.01 and AG 9700B), and comply with State and Federal law.

4.17.6. Use of online content for commercial and financial gains for any user is prohibited.

4.17.7. Under no circumstances is staff member online content delivery to be used to post student progress reports, grades, class assignments, or any other similar class-related material. The Board maintains its own systems (student information system such as Harmony that employees are required to use for the purpose of conveying information to students and/or parents.)

4.18. School provided devices, technology, networks, and software contained on those networks and devices are property of the Corporation.

4.19. User shall not copy school software for their personal use or for the use of others, except where expressly permitted under software license.

4.20. In addition, users may not copy software on any Corporation computer and may not bring software from outside sources for use on Corporation equipment without the prior approval of the Superintendent and Technology Staff.

4.21. Staff members retain rights of communication for collective bargaining purposes and union organizational activities.

5. Violations

5.1. The technology protection measures may not be disabled at any time that students may be using the network and/or school provided device, if such disabling will cease to protect against access to materials that are prohibited under the Children's Internet Protection Act.

5.2. Violations may include, but are not limited to:

5.2.1. Any user who attempts to disable the technology protection measures.

5.2.2. Unauthorized access to systems, including accessing another user's account without explicit permission and administrative approval.

5.2.3. Transmission or sharing of illegal material, such as confidential information, copyrighted material, obscene material, and harmful software.

5.2.4. Alteration of data, configuration, or files of another user without explicit consent.

5.2.5. Inappropriate sharing of information that is protected, such as student personally identifiable information, using sharing functionality.

5.2.6. Use of online services for irresponsible or inappropriate behavior online, whether alone or collaboratively within groups.

5.2.7. Recording and use of a camera and/or microphone in the following situations:

5.2.7.1. In inappropriate areas, such as restrooms, locker rooms, and other private meeting spaces.

5.2.7.2. Inappropriate sharing of recorded video.

5.2.7.3. Use of video for bullying.

5.2.7.4. Display of suggestive or explicit content ("sexting").

5.2.7.5. Recording and sharing of students that do not have permission to be photographed.

5.2.7.6. Any use of the camera and/or mic that is not educational or collaborative in nature.

5.3. Use of Corporation technology that is in violation of any federal, state, or local law is strictly prohibited.

5.4. Users who disregard this policy and its accompanying guidelines may have their use privileges suspended or revoked, and disciplinary action taken against them.

5.5. Users granted access to the Internet through the school's network assume personal responsibility and liability, both civil and criminal, for uses of the technology not authorized by this Board policy and its accompanying guidelines.

5.6. The due process rights of all users will be respected in the event there is a suspicion of inappropriate use of the technology. Users have a limited privacy expectation in the content of their personal files and records of their online activity while connected to the network and/or using a school provided device.

5.7. In rare situations, such as imminent risk of harm to oneself or others, law enforcement may be contacted, if the Corporation deems the action necessary for the safety of the student(s) or others from imminent harm.

5.8. It is impossible to define every instance of violation to this policy, so it will be at the discretion of the school administration to use judgment as to what is a violation in any undefined instances that may arise.

6. Limitations

6.1. First, and foremost, the Corporation may not be able to technologically limit access to services through the Corporation's Internet connection to only those that have been authorized for the purpose of instruction, study and research related to the curriculum.

6.2. The Corporation is not responsible for the care, troubleshooting, and maintenance of a personal device. Technical support for personal devices is limited to assisting with connecting the device to the Corporation network and is on a best effort basis.

7. Enforcement

7.1. The Corporation utilizes software and hardware to monitor online activity of students to restrict access to pornographic and other material that is obscene, objectionable, inappropriate and/or harmful to minors. Nevertheless, parents and guardians are advised that a determined user may be able to gain access to services on the Internet that the Corporation has not authorized for educational purposes.

7.2. Monitoring may include, but is not necessarily limited to, visual observations of online activities during class sessions; use of specific monitoring tools to review browser history and search queries; review of network, server, and computer data; and use of classroom management software.

7.3. Communications online, such as email, chat, and document collaboration, are subject to monitoring and review at any time.

7.4. Building and district administrators are responsible for providing training so that Internet users under their supervision are knowledgeable about this policy and its accompanying guidelines.

7.5. The Board expects that staff members will provide guidance and instruction to students in the appropriate use of the technology.

7.6. All users (and their parents or legal guardians if they are minors) are required to sign a policy and pledge each year to abide by the terms and conditions of this policy and its accompanying guidelines.

8. Security

8.1. A separate protected and isolated wireless connection will be provided to allow staff with accounts and appropriate level of access to access the Internet with personal devices that will simultaneously protect the network and facilitate filtered access to the Internet.

8.2. Personal devices may not be able to connect to school resources, such as printers and servers, due to the extra safeguards in place to protect the network.

8.3. Email may be provided to users authorized to have accounts on the network. In the case of student email, if provided, email will be provided for academic purposes only and will be restricted to internal only and specific external sources (such as .edu and .gov domains).

8.4. Security systems are in place on the Corporation network to protect users from harmful and dangerous content and software. Removal or disabling of these security systems are expressly prohibited except by authorized technology staff.

9. Privacy

9.1. All school communication systems are the Corporation's property and are to be used primarily for business purposes.

9.2. The Corporation retains the right to access and review any of its communications systems or school provided devices.

9.3. Staff members should have no expectation that any information contained on such systems and devices is confidential or private.

9.4. Review of such information may be done by the Corporation with or without the staff member's knowledge.

9.5. The use of passwords does not guarantee confidentiality, and the Corporation retains the right to access information in spite of a password.

9.6. School communication systems are to be used for business purposes. Personal messages on these systems should be limited in accordance with the Superintendent's guidelines. Staff members are encouraged to keep their personal records and personal business at home.

9.7. Users are prohibited from sending offensive, discriminatory, or harassing messages using the school communication systems.

9.8. Review of communication system data will only be done in the ordinary course of business and will be motivated by a legitimate business reason. If a staff member's personal information is discovered, the contents of such discovery will not be reviewed by the Corporation, except to the extent necessary to determine if the Corporation's interests have

been compromised. Any information discovered will be limited to those who have a specific need to know that information.

9.9. The administrators and supervisory staff members authorized by the Superintendent have the authority to search and access information electronically.

Responsible Use Away from School

10. Purpose

10.1. School provided devices that are permitted to be taken outside of school (such as home) with students and staff, such as but not limited to those offered in a one-to-one (1 to 1) environment, are intended for the same purposes as though those devices were on school premises (see Section 1).

10.2. School provided devices are for the sole purpose of educational use outside of school.

11. Scope

11.1. This policy applies to all school provided devices taken outside of school.

12. Requirements

12.1. The Corporation has implemented the use of technology protection measures which are specific technologies that will protect against (e.g. filter or block) access to visual displays/depictions that are obscene, pornographic, and other materials harmful to minors, as defined by the Children's Internet Protection Act including when the device is not at school.

12.2. Parents are advised and encouraged to:

12.2.1. Be involved with their child or children's online activities.

12.2.2. Provide additional supervision to ensure safe online activity.

12.2.3. Emphasize responsible use of technology.

13. Responsibilities

13.1. Students and staff are subject to the same responsibilities as though their school provided devices were on school premises (see Section 4).

13.2. Therefore, technology protection measures will remain in place to help protect students and staff online, and attempts to disable or circumvent those protection measures are subject to discipline.

13.3. Just as with textbooks, school provided devices are property of the Corporation and require the same high level of care as though those devices are on school premises. School provided devices taken home are for the sole purpose of providing the student use of technology for learning outside of school.

13.4. Use of online services outside of school must continue to serve their educational purpose and not be used for irresponsible or inappropriate behavior online, whether alone or within groups.

13.5. The device is not to be used by anyone except the student to whom it has been assigned.

13.6. The device is not a substitute for general home personal computing.

13.7. School provided devices that are determined to be damaged, whether intentionally or accidentally, whether at school or away from school, are subject to repair or replacement costs and depends on whether a parent or guardian opted in for insurance coverage, if available. Costs for repair will differ depending on the type of damage and may differ in a variety of situations, since technology devices are complex.

13.8. Administration, with the assistance of technology staff, will determine the associated costs for repair or replacement based on an assessment of the damage and repair or replacement costs.

13.9. Defects in the device not caused by damage are not subject to repair or replacement costs. Such a defect may include a factory defect discovered after devices are issued.

13.10. A building administrator will make the determination on the disposition of whether a device is damaged or defective. A single appeal can be made to a designated district administrator, if the disposition of the device is in dispute.

14. Limitations

14.1. Despite all efforts to protect users online, it is not possible for the Corporation to limit access to only content that has been authorized for the purpose of instruction, study and research related to the curriculum, even outside of school.

14.2. The Corporation is not obligated to provide technical support outside of school premises during or after hours. Problems with the school device should be brought to the Corporation's attention during the next regular school day.

14.3. Students are expected to know how to connect and disconnect from wireless connections ("hot spots"). Many wireless connections are secured and require a password in order to

connect successfully. The Corporation does not know the password to the wireless connection of another entity or household and therefore cannot assist. Please contact the provider of the wireless connection for further assistance.

15. Enforcement

15.1. All school provided devices outside of school are subject to monitoring as though the devices are on school premises.

15.2. Traffic to and from school provided devices are captured as part of the technology protection measures that are in place to allow approved content and block unapproved content.

15.3. School owned devices are subject to monitoring and review at any time.

15.4. Use of the camera and microphone for remote monitoring purposes is prohibited.

15.5. The location (such as GPS data) of the device may be used in the event a device is lost or stolen.

16. Violations

16.1. Students who are violating this policy when using a school provided device off of school premises will be subject to discipline as though the incident occurred on school premises (see Section 5).

16.2. The parent(s) or guardian(s) of the student will be informed of the incident.

16.3. In rare situations, such as imminent risk of harm to oneself or others, law enforcement may be contacted, if the Corporation deems the action necessary for the safety of the student(s) or others from imminent harm, even outside of school.

17. Security

17.1. Due to security measures in place on school provided devices, such devices may not be able to communicate with personal devices such as printers or computers away from school.

17.2. Email access, if provided, will continue to be restricted just as it is at school.

17.3. Use of personal accounts to log into school provided technology will not be allowed.

18. Privacy

18.1. Privacy of data on school provided devices will be the same as though those devices were at school (see Section 9).

18.2. Remote access by school personnel to personal networks where school provided devices may connect is outside of the scope of the Corporation and is not permitted. The privacy and security of home personal networks and 3rd party networks are respected.

Policy References

47 C.F.R. 54.520, Children's Internet Protection Act
15 U.S.C. 6501–6506 Children's Online Privacy Protection Act of 1998, as amended (2013)
18 U.S.C. 1460 Possession with intent to sell, and sale, of obscene matter on Federal property
18 U.S.C. 2246 Sexual abuse
18 U.S.C. 2256 Child pornography
20 U.S.C. 6801 et seq., Part F, Elementary and Secondary Education Act of 1965, as amended (2003)
20 U.S.C. 1232g; 34 CFR Part 99 Federal Education Rights and Privacy Act
20 U.S.C. 6777, 9134 (2003) Internet Safety and implementation of Children's Internet Protection Act
47 U.S.C. 254(h), (1), Communications Act of 1934, as amended (2012) Protecting Children in the 21st Century Act Amendment
76 F.R. 56295, 56303 Universal Service Support and certification for Schools and Libraries