Williston School District 29 Internet Safety Measures Meeting

October 20, 2015
District Office Auditorium

Erate applicants must enforce a policy of Internet safety and certify compliance the Children's Internet Protection Act (CIPA) to be eligible for discounts. CIPA was signed into law on December 21, 2000. To receive support for Internet Access, Internal Connections, and Basic Maintenance services from the universal service fund (USF), school and library authorities must certify that they are enforcing a policy of Internet safety that includes measures to block or filter Internet access for both minors and adults to certain visual depictions. The relevant authority with responsibility for administration of the eligible school or library (hereinafter known as the Administrative Authority) must certify the status of its compliance for the purpose of CIPA in order to receive USF support.

In general, school and library authorities must certify either that they have complied with the requirements of CIPA; that they are undertaking actions, including any necessary procurement procedures, to comply with the requirements of CIPA; or that CIPA does not apply to them because they are receiving discounts for telecommunications services only. **CIPA (Child Internet Protection Act)**

Public Notice and Hearing or Meeting

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing or meeting to address a proposed technology protection measure and Internet safety policy. (For private schools, "public" notice means notice to their appropriate constituent group.) Unless required by local or state rules, an additional public notice and a hearing or meeting is not necessary for amendments to Internet safety policies.

Williston School District 29 has technology protection measures in place along with and Internet Safety Policy.

At this time, Williston School District 29 uses Lightspeed Systems for content filtering of all inappropriate materials and websites. (http://www.lightspeedsystems.com/)

We also use Airwatch Mobile Device Management System to monitor company owned tablet devices.

Internet Safety Policy

Schools and libraries receiving universal service discounts are required to adopt and enforce an Internet safety policy that includes a technology protection measure that protects against access by adults and minors to visual depictions that are obscene, child pornography, or — with respect to use of computers with Internet access by minors — harmful to minors.

The Internet safety policy must address all of the following issues:

- Access by minors to inappropriate matter on the Internet and World Wide Web
- The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications
- Unauthorized access including "hacking" and other unlawful activities by minors online
- Unauthorized disclosure, use, and dissemination of personal information regarding minors
- Measures designed to restrict minors' access to materials harmful to minors

For schools, the policy must also include monitoring the online activities of minors. Note: beginning July 1, 2012, when schools certify their compliance with CIPA, they will also be certifying that their Internet safety policies have been updated to provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness, and response.

The following link is used to educate our children in regard to expectations put out by CIPA.

Educational presentations that are age appropriate from

http://www.Netsmartz.org

Internet Safety Policy

Policy IJNDB Use of Technology Resources in Instruction

Issued 4/12

Purpose: To establish the board's vision and the basic structure for the use of technology resources in instruction.

Technology is a vital part of education and the curriculum of the school district. In an effort to promote learning and expand educational resources for students, the district will provide access to technology resources contingent upon adherence to this policy, administrative rules and related guidelines. The school district will provide students and employees with access to the district's technology resources including, but not limited to, computer systems, media and peripheral devices.

Access to the district's technological resources is a privilege, not a right. With this privilege, there also is a responsibility to use the resources solely for educational purposes and not to access inappropriate materials. The district's technology resources have specific educational purposes that include use for classroom activities, professional or career development and administrative functions. The faculty will thoughtfully integrate use of technology throughout the curriculum and will provide guidance and instruction to students in its use.

In order to achieve proper implementation of the district's technology resources and prior to accessing the ⏩Internet⏪, students and staff will receive instruction annually on the technology acceptable use ⏩policy⏪ and guidelines which include the appropriate use of the ⏩Internet⏪ and ⏩Internet⏪ ⏩safety⏪ measures. Users must adhere to strict guidelines developed by the administration to govern the use of district computers. These guidelines are provided so that all users are aware of their responsibilities. Violations of these guidelines will not be tolerated and will subject the user to appropriate disciplinary action.

There are many risks -- known and unknown -- associated with technology use, particularly the use of the Internet, e-mail and related electronic communications. Such risks include unauthorized access by others to one's personal information, computer hacking, fraud, defamation, exposure to harmful materials (e.g., those that are pornographic, obscene, threatening, violent, abusive or otherwise improperly offensive), financial exploitation and conveying inaccurate, provocative or false information.

Officials of the district will strive to take all reasonable measures to minimize these risks for users and will provide users with instruction and guidelines to assist them. For instance, the district provides content filtering capabilities to comply with federal regulations pursuant to the Children's Internet Protection Act and E-rate provisions. Because Internet filtering and spam blocking controls are imperfect, they cannot block all undesirable content or protect against all risks. Likewise, they may inadvertently block access to educationally appropriate and valuable information. Users, therefore, assume these risks for themselves when they use district technology resources.

The district reserves the right to disclose any user's electronic communications or data to district or non-district personnel or agencies to the extent permitted or required by law. The Internet

sites viewed or the e-mails sent by users may be public records subject to disclosure. Regardless of whether such uses generate public records, the district has the right to review and monitor all uses of its technology resources. The superintendent or his/her designee will maintain a system for the securing, cataloging and storing of all records that is in compliance with state and federal laws.

The district does not offer any warranty against defect or damage to users of its technology resources. The district is not responsible for damages or losses suffered by users, including loss of data resulting from delays, disruptions or other causes. Furthermore, the district provides no assurance regarding the accuracy or quality of information obtained through such resources, particularly via email or the Internet.

Students must sign a form acknowledging that they have read, or had read to them, and understand the technology acceptable use policy and guidelines; that they will comply with the policy and guidelines; and that they understand the consequences of violating the policy or guidelines. In addition, parents/legal guardians will be required to sign a technology acceptable use permission form before students will be allowed use of technology resources. Teachers and school and district staff must sign a similar acknowledgment form that they have read, understand and will comply with the district's technology acceptable use policy and administrative rules.

Student Internet activities will be monitored by the district to ensure students are not accessing inappropriate sites that have visual depictions that include obscenity, child pornography or are harmful to minors. The district will use technology protection measures to protect students from inappropriate access.

District and school computer technicians who are working with a computer and come across sexually explicit images of children must report this to the local law enforcement and the superintendent. The report must include the name and address of the owner or person in possession of the computer.

The district will provide reasonable notice of and at least one public hearing or meeting to address and communicate its Internet safety measures.

Online behavior

The district will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The superintendent or his/her designee will develop a program to educate students on these issues.

Off-campus Internet conduct

Teachers, staff, students and parents/legal guardians should understand that the district may take disciplinary action for off-campus conduct involving inappropriate use of the Internet or Web based resources if that conduct results in a disruption of the school environment. The school or district may take disciplinary action when there is inappropriate off-campus conduct such as posting online comments that intimidate, bully, harass or threaten other students or staff members or that have a negative impact on the school environment. Such conduct is not limited to textual comments and may include, but not be limited to, the inappropriate use of photos, pictures or other visual materials that harass or threaten others or create a negative impact on the

school environment.

Adopted 2/18/98; Revised 10/20/09, 4/24/12

Legal references:

Federal law:

47 USC Section 254(h) - Children's Internet Protection Act.

The Digital Millennium Copyright Act of 1998, Section 512 - Limitations on liability relating to material online.

S.C. Code of Laws, 1976, as amended:

Section 10-1-205 - Computers in public libraries; regulation of Internet access.

Section 16-3-850 - Encountering child pornography while processing film or working on a computer.

Section 16-15-305 - Disseminating, procuring or promoting obscenity unlawful; definitions; penalties; obscene material designated contraband.

Section 59-19-90 - General powers and duties of school trustees.

Court cases:

Purdham v. Fairfax Co. Sch. Bd., 637 F.3d 421, 427 (4th Cir. 2011).

Technology Use Guidelines

I. Introduction

Each employee, student or non-student user of Williston School District 29 (WSD29) information system is expected to be familiar with and follow the expectations and requirements of this administrative rule. The purpose of this rule is to ensure that individuals are aware of their responsibilities regarding the Internet and related technology and equipment. This rule also helps ensure the safety and privacy of current and former employees and students.

A. Legal Requirements

WSD29 is committed to complying with applicable information security requirements and relevant information security standards and protocols. These requirements include, but are not limited to the following:

1. The Family Educational Rights and Privacy Act (FERPA)
2. Children's Internet Protection Act (CIPA)
3. Individuals with Disabilities Education Act (IDEA)
4. Children's Online Privacy Protection Act (COPPA)
5. Health Insurance Portability and Accountability Act (HIPPA)

Users of WSD29's network are required to adhere to state and federal law as well as board policy. Any attempt to break those laws or policies through the use of WSD29 networks may result in discipline or litigation against the offender(s) by the proper authority. WSD29 will provide any information necessary in order to fully cooperate with the appropriate authorities in the civil and/or criminal process.

B. Acceptable Use

WSD29 provides computer, network, e-mail, and Internet access to individuals as part of the learning environment. The use of these resources is a privilege and not a right. While these systems have the power to deliver a vast number of resources to classrooms and enhance education, their effectiveness depends on the responsible and ethical use by every individual. Violation of this administrative rule will result in the loss of this privilege and may result in discipline or litigation in accordance with board policy and state and federal law.

II. Employee Acceptable Use

This section is dedicated to provide WSD29 employees with guidance of acceptable use of the District's information technology resources, including but not limited to:

1. The internet, intranet, e-mail, portal
2. District assigned computing devices such as phones, tablets, ipads, laptops, desktops or any other type of electronic devices and
3. The District's network and supporting systems and data transmitted by and stored on the WSD29 systems.

A. Annual Responsibilities and Information Security Awareness

Staff members will review the Information Security Awareness materials presented annually.

B. Prohibited Use of WSD29 Resources

The following uses of WSD29 computer resources by staff members are prohibited at all times:

1. Unauthorized or excessive personal use. Any personal use should not interfere with or impair an employee's job performance.
2. Infringing upon the intellectual property rights of others or violating copyright laws.
3. Advancing personal profit.
4. Furthering political causes in violation of board policy or the State Ethics Act.
5. Uploading or transferring out of the District's direct control any software licensed to the District or data owned by the District without explicit written authorization. Failure to observe copyright or license agreements can result in disciplinary action from WSD29 or legal action by the copyright owner.
6. Unauthorized use of resources (including but not limited to servers, networks, computers and printed output) to reveal confidential or sensitive information, student data, or any other information covered by existing state or federal privacy or confidentiality laws, regulations, rules, policies, procedures, or contract terms.
7. Downloading software unless it is required to complete their job responsibilities and approved and implemented by Technology Services (TS).
8. Bypassing or attempting to bypass any of the District's security or content filtering safeguards.
9. Accessing or attempting to access resources for which an employee does not have explicit authorization by means of assigned user accounts, valid passwords, file permissions or other legitimate access and authentication methods.
10. Granting another individual access to any District accounts that have been authorized to you or using another individual's District authorized accounts, user-id's and/or passwords. Specific exceptions are allowed for Technology Services personnel for authorized system operations and maintenance.
11. Allowing another person to use a District system under his or her login.
12. Adding, modifying, repairing, removing, reconfiguring, or tampering with any device on the network infrastructure.

13. Allowing non-district persons permission to use District assigned information systems on District equipment taken off-site.
14. Sharing the password of their unique WSD29 user ID.

15. The use of any "hacking tools" that can be used for "computer hacking", as defined in the South Carolina Computer Crime Act, may not be possessed on school property, on any District premise, or run or loaded on any District system.

16. Violating any state or federal law or regulation, board policy or administrative rule.

C. Sensitive Information

WSD29 employees who have or may have access to personally identifiable student records shall adhere to all standards included in the Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPPA), Children's Online Privacy Protection Act (COPPA), and other applicable laws and regulations, as they relate to the release of student information.

1. Employees may not disclose sensitive or personally identifiable information regarding students to individuals and/or parties not authorized to receive it. Authorization to disclose information of a student to individuals and/or parties must strictly adhere to regulations set forth in the FERPA - *See Board Policy and Administrative Rule JR.*
2. Information contained in these records must be securely handled and stored according to WSD29 directives, rules and policies and if necessary destroyed in accordance with state information retention standards and archival policy.

D. Granting Access to Secure Locations

Staff members may only grant access to sensitive and secure areas, including but not limited to, server rooms and wire closets, after verification with TS of the credentials and need for access of the person requesting access.

E. Limited Personal Use

WSD29 does not grant any ownership, privacy or an expectation of privacy in the contents of any message, including email, or other Internet activities involving WSD29 resources or equipment.

Personal use is prohibited if:

1. It interferes with the use of IT resources by the District;
2. Such use burdens the District with additional costs;
3. Such use interferes with the staff member's employment duties or other obligations to the District; or
4. Such use includes any activity that is prohibited under any district (including this rule), board policy, or state or federal law.

F. Email Maintenance

Each District e-mail user is responsible for the content of all text, audio, or image that he or she places or sends over the Internet or District email systems.

1. Emails will only be backed up for fourteen calendar days, and each employee will be limited to a total of 25GB of message storage space. Employees must delete messages they don't need or store messages that they will need in another way besides the electronic mail system. Examples of storing emails are printing, saving to other document types or archiving messages in off-line email folders. An employee must preserve all emails and other relevant records related to an incident that is subject to litigation once that employee is made aware of the legal action.
2. Email messages are considered public records and may be released pursuant to the requirements of the South Carolina Freedom of Information Act.

G. Consequences

Employees who violate this administrative rule may be subject to discipline, including up to termination. All employees are responsible for reporting breaches and possible breaches of security. Incidents should be reported to an employee's supervisor and directly to Technology Services (TS). Suspected criminal activity must be immediately reported to law enforcement.

III. WSD29 Internet Safety and Other Terms of Use

A. General Access

In compliance with the Children's Internet Protection Act ("CIPA"), U.S.C. §254 (h), the District uses technological devices designed to filter and block the use of any of the District's computers with Internet access to retrieve or transmit any visual depictions that are categorized as obscene, child pornography, or "harmful to minors" as defined in the CIPA.

1. Though the District makes reasonable efforts to filter such Internet content, the District cannot warrant the effectiveness of its Internet filtering due to the dynamic nature of the Internet.
2. Users of a District computer with Internet access may request that the "technology protection measures" be temporarily disabled to conduct bona fide research for another lawful purpose. These requests should be made to TS with the knowledge of that employee's supervisor.

B. Education, Supervision, and Monitoring

It shall be the responsibility of all District school staff to make a reasonable effort to educate, supervise, and monitor appropriate usage of online computer network access to the Internet in accordance with this administrative rule, CIPA, COPPA, and the Protecting Children in

the 21st Century Act.

C. Personal Safety

The following list is considered precautions taken by WSD29 to ensure the safety of their students, employees, and other individuals.

1. Students will not post or email personal contact information about themselves or other people unless it is in conjunction with a specific teacher-approved assignment or approved college/career communication.
2. Students will not agree to meet with someone they have met online without their parent/guardian's approval.
3. Students will promptly disclose to an administrator, teacher, or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.
4. Employees will report any concerns related to their use of technology to their immediate supervisor.

D. Education, Supervision, and Monitoring

It shall be the responsibility of all District school staff to make a reasonable effort to educate, supervise, and monitor appropriate usage of online computer network access to the Internet in accordance with this administrative rule, CIPA, COPPA, and the Protecting Children in the 21st Century Act.

E. Expectation of Privacy

Individuals should not have an expectation of privacy in the use of the District's email, systems, or equipment. The District may, for a legitimate reason, perform the following:

1. Obtain emails sent or received on District email.
2. Monitor an individual's use on the District's systems.
3. Confiscate and/or search District-owned software or equipment.
   The District may confiscate and search personal electronic devices in accordance with *New Jersey v. T.L.O.* and applicable law.

F. Acknowledgement

This Acceptable Use Agreement applies to all digital technologies and environments, including (although not limited to):

- school owned ICT devices (e.g. desktops, laptops, printers, scanners)
- mobile phones and student owned devices
- email and instant messaging
- internet, intranet
- social networking sites (e.g. Facebook)
- video and photo sharing websites (e.g. YouTube)
- blogs or micro-blogs (e.g. Twitter)
- forums, discussion boards and groups (e.g. Google groups)

- wikis (e.g. Wikipedia)
- vod and podcasts
- video conferences and web conferences.

This Acceptable Use Agreement applies when digital technologies are being used at school, during school excursions, at camps and extra-curricular activities, and at home.

Technology Use Guidelines (Employee)

Signature:

I understand and agree to comply with the terms of acceptable use and expected standards of behavior set out within this agreement.

I understand that there are actions and consequences established within the school's Student Engagement Policy if I do not behave appropriately.

Employee name: _____

Employee signature: _____

Location: _____

Date: _____

Technology Use Guidelines

III. Introduction

Each employee, student or non-student user of Williston School District 29 (WSD29) information system is expected to be familiar with and follow the expectations and requirements of this administrative rule. The purpose of this rule is to ensure that individuals are aware of their responsibilities regarding the Internet and related technology and equipment. This rule also helps ensure the safety and privacy of current and former employees and students.

C. Legal Requirements

WSD29 is committed to complying with applicable information security requirements and relevant information security standards and protocols. These requirements include, but are not limited to the following:

1. The Family Educational Rights and Privacy Act (FERPA)
2. Children's Internet Protection Act (CIPA)
3. Individuals with Disabilities Education Act (IDEA)
4. Children's Online Privacy Protection Act (COPPA)
5. Health Insurance Portability and Accountability Act (HIPPA)

Users of WSD29's network are required to adhere to state and federal law as well as board policy. Any attempt to break those laws or policies through the use of WSD29 networks may result in discipline or litigation against the offender(s) by the proper authority. WSD29 will provide any information necessary in order to fully cooperate with the appropriate authorities in the civil and/or criminal process.

D. Acceptable Use

WSD29 provides computer, network, e-mail, and Internet access to individuals as part of the learning environment. The use of these resources is a privilege and not a right. While these systems have the power to deliver a vast number of resources to classrooms and enhance education, their effectiveness depends on the responsible and ethical use by every individual. Violation of this administrative rule will result in the loss of this privilege and may result in discipline or litigation in accordance with board policy and state and federal law

Technology Use Guidelines (Student)

II. Student Acceptable Use

This section is dedicated to provide WSD29 students with guidance of acceptable use of the district's information technology resources, including but not limited to:

1. The internet, intranet, e-mail, portal;
2. District assigned computing devices such as phones, tablets, ipads, laptops, desktops, electronic devices, BYOD devices and portable storage; and
3. The District's network and supporting systems and data transmitted by and stored on these systems.

A. Compliance with Copyright Laws

Students shall follow copyright laws at all times. Students should refer all questions regarding copyright concerns to administrators at their school.

B. Filtering and Monitoring Computer Resources

The District takes reasonable precautions by using filtering software to keep inappropriate Internet sites and e-mail out of the classroom. The District strongly adheres to the guidelines set forth by COPPA and CIPA when installing filtering/monitoring software devices on District equipment. The District does not supervise individual e-mail accounts.

1. The District reserves the right to review any e-mail sent or received using District equipment and e-mail accounts.
2. Students must adhere to the behavior expectations while using technology and e-mail, including but not limited to those expectations contained in board policy. The District's Board Policy is JICJ/Possession/Use of Electronic Communication Devices and IJNDB/Use of Technology Resources in Instruction.
3. Technology is constantly changing and evolving. Due to the nature of the Internet, online communications, and evolving technology, the District cannot ensure or guarantee the absolute safety of students during the use of technology, including email and the Internet. Parents and students should contact the school immediately with any concerns related to the use of technology.

C. Prohibited Uses of WSD29 Resources

The following uses of WSD29 computer resources by students are prohibited from:

1. The use of school computers for commercial purposes.
2. The use of obscene, bullying, profane, lewd, threatening, disrespectful, or gang related language or symbols.

3. The bypass or attempt to bypass any of the District's security or content filtering safeguards.
4. Allowing another person to use the computer under your District login.
5. Adding, modifying, repairing, reconfiguring or otherwise tampering with any device on the network infrastructure including, but not limited to: wireless network devices, computers, printers, servers, cabling, switches/hubs, routers, etc.
6. Unauthorized access, overloading, more commonly known as Distributed Denial of Service or Denial of Service, or use, or attempted unauthorized access or use of District information systems.
7. Destroying or tampering with any computer equipment or software.
8. The use of any "hacking tools" that can be used for "computer hacking", as defined in the South Carolina Computer Crime Act, may not be possessed on school property, on any District premise, or run or loaded on any District system.
9. The use of any "hacking tools" that can be used for "computer hacking", as defined in the South Carolina Computer Crime Act, may not be possessed on school property, on any District premise, or run or loaded on any District system.
10. The use of school computers for illegal activities including but not limited to planting viruses, hacking, or attempted unauthorized access to any system.
11. Violating any state for federal law or regulation, board policy or administrative rule.

D. Agreement of Use

Students, parents and guardians agree that WSD29 computer equipment must be handled with care and respect.

E. Consequences

Students who violate this administrative rule may be subject to disciplinary action up to and including expulsion in accordance with board policy and state and federal law. Suspected criminal activity must be immediately reported to law enforcement.

IV. WSD29 Internet Safety and Other Terms of Use

G. General Access

In compliance with the Children's Internet Protection Act ("CIPA"), U.S.C. §254 (h), the District uses technological devices designed to filter and block the use of any of the District's computers with Internet access to retrieve or transmit any visual depictions that are categorized as obscene, child pornography, or "harmful to minors" as defined in the CIPA.

1. Though the District makes reasonable efforts to filter such Internet content, the District cannot warrant the effectiveness of its Internet filtering due to the dynamic nature of the Internet.
2. Users of a District computer with Internet access may request that the "technology protection measures" be temporarily disabled to conduct bona fide research for another lawful purpose. These requests should be made to TS with the knowledge of that employee's supervisor.

H. Education, Supervision, and Monitoring

It shall be the responsibility of all District school staff to make a reasonable effort to educate, supervise, and monitor appropriate usage of online computer network access to the Internet in accordance with this administrative rule, CIPA, COPPA, and the Protecting Children in the 21st Century Act.

I. Personal Safety

The following list is considered precautions taken by WSD29 to ensure the safety of their students, employees, and other individuals.

1. Students will not post or email personal contact information about themselves or other people unless it is in conjunction with a specific teacher-approved assignment or approved college/career communication.
2. Students will not agree to meet with someone they have met online without their parent/guardian's approval.
3. Students will promptly disclose to an administrator, teacher, or other school employee any message they receive that is inappropriate or makes them feel uncomfortable.
4. Employees will report any concerns related to their use of technology to their immediate supervisor.

J. Education, Supervision, and Monitoring

It shall be the responsibility of all District school staff to make a reasonable effort to educate, supervise, and monitor appropriate usage of online computer network access to the Internet in accordance with this administrative rule, CIPA, COPPA, and the Protecting Children in the 21st Century Act.

Technology Use Guidelines (Student)

K. Expectation of Privacy

Individuals should not have an expectation of privacy in the use of the District's email, systems, or equipment. The District may, for a legitimate reason, perform the following:

1. Obtain emails sent or received on District email.
2. Monitor an individual's use on the District's systems.
3. Confiscate and/or search District-owned software or equipment.
   The District may confiscate and search personal electronic devices in accordance with *New Jersey v. T.L.O.* and applicable law.

L. Acknowledgement

This Acceptable Use Agreement applies to all digital technologies and environments, including (although not limited to):

- school owned ICT devices (e.g. desktops, laptops, printers, scanners)
- mobile phones and student owned devices
- email and instant messaging
- internet, intranet
- social networking sites (e.g. Facebook)
- video and photo sharing websites (e.g. YouTube)
- blogs or micro-blogs (e.g. Twitter)
- forums, discussion boards and groups (e.g. Google groups)
- wikis (e.g. Wikipedia)
- vod and podcasts
- video conferences and web conferences.

This Acceptable Use Agreement applies when digital technologies are being used at school, during school excursions, at camps and extra-curricular activities, and at home.

Technology Use Guidelines (Student)

I understand and agree to comply with the terms of acceptable use and expected standards of behavior set out within this agreement.

I understand that there are actions and consequences established within the school's Student Engagement Policy if I do not behave appropriately.

Student name: _____

Student signature: _____

Parent Signature: _____

School: _____

Date: _____

[1]

[1] Updated 10-31-2016