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.

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.

Technology Use Guidelines (Student)

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.

Technology Use Guidelines (Student)

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 (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: _____