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.

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 (Employee)