WASHINGTON UNIFIED SCHOOL DISTRICT
FACULTY AND STAFF ACCEPTABLE USE PROCEDURES/ INTERNET AND EMAIL ACCESS PROCEDURES

I. Overview and Purpose

This document contains the Acceptable Use /Internet and Email Access Procedures for faculty and staff for the Washington Unified School District (WUSD) derived from Board Policy. These policies govern the use of network and electronic tools and media for all WUSD employees.

Washington USD provides Internet access to all students and staff. Internet access allows classrooms and individuals to have access to information, software, news and opinion, and communication by electronic mail that originates from any point in the world. Our goal is to promote educational excellence by facilitating resource sharing, innovation and communication within our own community and the world. The District also seeks to protect its employees, students and the schools from illegal or damaging actions by individuals, either knowingly or unknowingly.

DIRECTIONS: Faculty and staff should read this entire document carefully, then sign and date the accompanying *Acknowledgement of Receipt* and return it to the appropriate supervisor.

For the purpose of these procedures, technology is defined as, but not limited to the following:

a. All workstations (both desktop and portable), printers, scanners and other peripherals;
b. Learning resource management systems, including library automation systems;
c. Distance learning systems;
d. Video capturing, broadcast, receiving, and distribution systems;
e. Teleconferencing systems;
f. All software;
g. Office copier, imaging, and document management systems that would be connected to computer network;
h. Cameras, whiteboard systems and peripherals; and
i. Web-based subscription software packages.

Faculty and staff members may access the Internet for educational or work-related purposes at any time which is not disruptive and does not interfere with the performance of other responsibilities of the user or other staff members. Faculty and staff should expect only limited privacy of the contents of any files on the District computer system. Routine maintenance and monitoring may lead to the discovery that faculty and staff have violated policies/rules addressed herein, or state/federal laws. If a violation is found, an investigation will follow that will be reasonable and related to the violation. An employee who violates the terms of this administrative rule or otherwise misuses the Internet to access inappropriate material may be subject to disciplinary action.

II. General Use Guidelines

Please read the following carefully.

1. The WUSD network and technology may not be used for commercial purposes, financial gain, a personal business, product advertisement or political lobbying activities (BP 1160).

2. Caring for computer equipment is a serious issue. Objects should not be placed on monitors, computers, or keyboards. Food and beverages should not be used in the vicinity of computers.

3. The contents of any device used on the District computer system may be monitored [e.g. jump drives, CDs, digital cameras and other such device] and are subject to scanning by the District's

scanning software. Employees should be aware that files are subject to destruction if found to contain virus or malware. All data should be stored on my Home Directory that is on the network. If a workstation has to be re-imaged, all data stored on the hard drive will be lost. Users should be aware that the content they create on the school district systems remains the property of WUSD.

4. Bargaining Units may use District technology to notify members of meetings and to survey their members. Communication from the individual members to their elected Association representatives must be done on an individual basis.

5. No user will attempt to gain unauthorized access to the electronic network or to any other computer systems through the electronic network or go beyond authorized access. This includes attempting to log in through another person's account or access another person's files. No user will attempt to disrupt the computer system or destroy data by any other means such as spreading computer viruses. Deliberately deleting/destroying any computer programs, systems, or data files is not permitted. Do not search for security problems in the electronic network; this will be considered as an illegal attempt to gain access.

6. Each individual user is responsible for his or her individual account and should not provide his or her password to another person, including students. This information should not be publicly displayed. Users will not provide system access to unauthorized individuals, especially non-employees of the District. If a user logs onto the computer network using an individual password, the individual should log off the network when he leaves the workstation. Use of the District's email accounts from any location falls under the same guidelines.

7. As such, work stations assigned and/or designated to staff are intended for staff use only. Faculty and staff members will log on to the network only as themselves, and are responsible for their individual accounts and will take all reasonable precautions to prevent others from being able to use their accounts or access locally stored documents. Staff computers contain sensitive information and give access to items like student records and grading. Faculty and staff members will immediately notify the Technology Department if they suspect that there is a possible security problem.

8. Users will not use any District technology to access, create, print, post, or download materials that would not be permissible in WUSD in any form (i.e., obscene, profane, or pornographic materials; sexting; materials that use language or images that are inappropriate in the education setting or disruptive to the educational process; materials that use language or images that advocate violence or discrimination toward other people or that may constitute harassment, discrimination or threatens the safety of others; shopping online during time designated as work time by the District, unless in the performance of their duties for the district; storage of personal photos, videos, music or files not related to educational purposes for any length of time during designated work times). (BP 4040; AR 1114)

9. Observe all copyright rights of owners and follow all expressed requirements. If unsure whether or not one can use a work, one should request permission from the copyright owner (BP 6162.6).

10. Use of the network for any illegal activities is prohibited. Illegal activities include, but are not limited to: tampering with computer hardware or software; software piracy; unauthorized entry into computers and files (hacking); knowledgeable vandalism or destruction of equipment. Such activity is considered a crime under state and federal law. Users must be aware that any illegal action carried out over the Internet will be reported to law enforcement officials for possible prosecution. Please be advised, it is a federal offense (felony) to break into any security system. Financial and legal consequences of such actions are the responsibility of the user (staff, volunteer, and student) and students' parent or guardian.

11. The District's electronic technologies will not be used to post information in public access areas regarding private or confidential information about another person, including student information. Private or confidential information is defined by board policy, state law, and federal law.

12. The use of anonymous proxies to get around content filtering is strictly prohibited and is a direct violation of this agreement.

13. Users shall neither download nor install any commercial software, shareware, or freeware onto any district device or network drives without prior permission of the Information Technology Department.

14. Users will not access restricted computer equipment, such as servers or locked cabinets with electronic equipment, without authorization.

15. There should be no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received on the school computer network or stored in the user's directory or on a disk drive.

16. The District is required by the Children's Internet Protection Act to use filtering software for all electronic devices to protect students from pornographic and otherwise harmful content in accordance with federal law. Filtering of such content is also applied to district employees for the protection of employees and the district.

17. The District makes no guarantee that the functions or the services provided by or through the District electronic network will be error-free or without defect. The District will not be responsible for any loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for any financial obligations arising from the unauthorized use of the system.

III. Email Account Guidelines:

1. WUSD provides email accounts for the express purpose of conducting school and district business. WUSD email accounts should be used to conduct school and district business. Use of outside personal email accounts should be limited throughout the school day.

2. All users are expected to use email in a professional, legal, and ethical manner.

3. Do not open attachments from an unknown person or source, or respond to spam, e.g. unsolicited junk mail or chain letters. Attachments can be the source of viruses.

4. Do not use inappropriate language in public or private messages, or in other material that may be accessed by others. Inappropriate language includes:
   a. Obscene, profane, lewd, vulgar, rude, inflammatory, threatening, or disrespectful language.
   b. Language that could cause damage, danger or disruption.
   c. Personal attacks, including prejudicial or discriminatory attacks.
   d. Harassment, or persistently acting in a manner that distresses or annoys another person.
   e. Posting false or defamatory information about a person or organization.
   f. Information pertaining to dangerous instruments such as bombs or other explosive devices, automatic weapons or other firearms, other weaponry.

5. WUSD monitors employee correspondence/email and reserves the right to inspect electronic mail and computer generated logs regarding web sites visited by users. If the District suspects violations of law, harassment of others or violation of other District policies, disciplinary action may be taken. Copies of all messages exist on other servers and workstations and are archived by the District.

IV. Social Networking Guidelines

These guidelines are for employees engaging in social networking for work related educational/instructional use (BP 4040; AR 1114):

1. Faculty and staff will create a separate social networking account (not connected to a personal account) when the intent is to interact with students for school-related purposes.

2. All rules apply from all areas outlined in this Acceptable Use Agreement.

3. Respect co-workers and students. Do not discuss students, their families or co-workers.

4. In the interests of protecting student privacy and safety, images of District students obtained from school related events may not be included on personal social networking sites.

5. Social media identifications, login identifications and user names must not contain the District's name or logo on personal networking sites.

V. Student Records / Information:

The Federal Family Educational Rights and Privacy Act defines who has access rights to student records. Parents and legal guardians do have rights; without parental permission, most others do not. School district personnel may have access without parental permission when they are acting as an education official with a legitimate interest.

Washington Unified School District (WUSD) employees have the following obligations with regard to student information and records:

- Do not disclose student records to anyone.
- Do not use the information you receive except for the purpose it was intended.

The Governing Board of WUSD has adopted two Board Policies relevant to student information confidentiality. Copies of these Board Policies are available in the Superintendent's Office:

- Board Policy 5300 Pupil Records – Confidentiality, addresses the District's responsibility to assure the security of pupil records

- Board Policy 3560.4 Food Services – Confidentiality Requirements, addresses the strict confidentiality of eligibility and participation in the free and reduced price meal program – most District employees are not authorized to have access to this information

Additionally, the following Education Codes apply to access of student records:

- Education Code 49064: Log of Persons and Organizations Requesting or Receiving Information
- Education Code 49069: Absolute Right to Access
- Education Code 49073: Release of Directory Information
- Education Code 49075: Access to Records by any Person with Written Parental Consent
- Education Code 49076: Access to Records by Persons without Written Parental Consent or Under Judicial Order
- Education Code 49077: Access to Information Concerning a Student in Compliance with Court Order; Notice to Parents and Pupil

In addition to District employee's responsibility to comply with the terms of the Family Education and Rights Privacy Act, and with the above named Board Policies and Education Codes, the following guidelines are to be followed by all WUSD employees with access to the student information system (AERIES):

- Students shall not have access of any kind to student information systems [i.e., Aeries, ABI, SEIS, and/or Data Director].
- No information shall be shared, even with other District employees that would interfere with the administration of a school (i.e., sharing student schedules prior to their release by the school).
- No user shall disclose his/her log-on or password with any other person.

- Long-Term Substitute employees shall be given access to internet, email, Aeries, and Data Director.
- SIS problems are to be addressed to the Help Desk email address.
- All discarded student records are to be shredded.

Washington Unified School District
Acceptable Use/Internet and Email Access Procedures
Acknowledgement of Receipt

I acknowledge that I have received the Acceptable Use/Internet and Email Access Procedures. These procedures and guidelines are derived from Board Policies that govern employee use of the Internet, network, electronic mail, and computing devices.

_____	_____
Signature of Staff Member	Date
_____	_____
Printed Name of Staff Member	School Site