TITLE: **ACCEPTABLE USE POLICY: ACCESS TO ELECTRONIC INFORMATION, SERVICES AND NETWORKS FOR DISTRICT EMPLOYEES**	NUMBER: **AR 3.3a(1e)**
***Executive Limitation**: EL 3, Treatment of Staff (3.3 – Employee Regulations)*	
Recorded as Administrative Regulation: *Established: 3/8/04 Revisions:11/24/08, 6/25/12, 5/27/15*	
Origin as Board Of Education Policy: *Established: n/a Revisions:*	

The District understands the importance of teachers, students and parents engaging, collaborating, learning, and sharing in digital environments. The District is committed to developing and providing technology resources that promote learning for students and staff and to facilitating resource sharing, content creation, collaboration, innovation and communication.

Technology use, whether the technology is owned by the District or the user, entails personal responsibility. The District expects that all staff and students will use technology in a responsible and ethical manner and in conformance with DASD Guiding Principles and Rules and all applicable laws. The District reserves the right to restrict or revoke access.

This Acceptable Use Policy is comprised of two (2) sections to govern staff decisions and behavior: Guiding Principles and Rules. For the purposes of these rules and guidelines, electronic information, network resources, and communication services include, but are not limited to: network services (both wired and wireless), hardware, (including printers and copiers), mobile devices, software, social media tools, learning management systems, Web 2.0 tools, telecommunications services, email services, and audio/video equipment.

<u>Guiding Principles</u>

1. Selecting Resources: The District's educational goals and administrative policies will be used as guides when selecting and appropriately using technology for assigned duties.
2. Communication Strategy: Electronic information, network resources and communication services may be used to inform and engage internal and external stakeholders, promote professional learning communities and personal learning networks, facilitate meaningful collaboration and student learning.
3. Representing the District & Yourself: When selecting images, signatures, and other similar elements for social media and communication services, staff should consider the District's educational goals and administrative policies.
4. Privacy: Network activity is monitored, logged, and reported regularly as part of Learning Information Systems operations. Use of the District's networks and communication resources should not be considered private. The District retains exclusive control of electronic information and resources. Records of network activity and resource use may be reviewed at the discretion of the District Administrator (or designee). Such reviews will be conducted as

necessary and may occur with or without notice, with or without consent, and without a search warrant.

5. Learning: Staff members are responsible for keeping current with District technology tools and maintaining a proficient level of technology skills.
6. Social Media: Staff should consult with the Technology Integrator, School/Community Relations Coordinator (SCR) or Learning Information Systems Coordinator (LIS) before using social media tools for professional purposes. The SCR and LIS departments will assist staff in developing appropriate uses for social media, selecting appropriate internal, online tools and/or public social media outlets, and helping define an instructional or communication strategy for using these tools.More information on guidelines for social media can be found on the District website: www.deforest.k12.wi.us/cms_files/resources/SocialMediaGuidelinesR8-25-11.pdf
7. Monitoring: Content on each of the District-sponsored social media sites will be monitored to ensure adherence to the social media guidelines for appropriate use, message and branding consistent with the goals of DASD.
8. Instructional Purpose: Information & images posted online or shared through social media should have an instructional purpose and must relate to curriculum and instruction, school-authorized activities, or information about the DeForest Area School District or its mission.
9. Communication: District employees are personally responsible for the content they publish online, including social media sites. Online behavior should reflect the same standards of honesty, respect, and consideration that are expected in face-to-face communication. The Board of Education has an overriding interest and expectation in deciding who may "speak" and what is "spoken" on behalf of the District on public social media sites. All official DASD presences on social media sites, online environments, or other electronic communication services are considered an extension of the District's information networks and are governed by this Handbook and this Acceptable Use Policy (AUP).
10. Personal Use: Employee use of District resources for personal use during work hours should be infrequent and incidental and should not intrude on or distract from the learning environment for students or the productivity of colleagues. Staff should be aware that any communication using District resources is subject to Wisconsin Public Records Laws.

<u>Rules</u>

1. System security: Users are responsible for the appropriate use and care of District provided electronic information and communication resources. Users shall not intentionally seek to modify or share data, passwords, information, hardware or resources belonging to other network users without permission. Unauthorized access or sharing of information may result in a revocation of privileges. This information includes records such as personnel records, medical records, identification numbers, account numbers, passwords, access codes, personal contact information and/or financial information. Unauthorized access or attempts to access another user's password, data, messages or other electronic communication system information is prohibited. Use of the District's electronic information and communication resources shall not disrupt the use of other users. District owned resources including data, devices, and files shall not be destroyed or abused in any way.
2. Personal account security: Staff members are responsible for keeping passwords secure. Staff accounts have increased privileges and access to private information concerning students, staff, and District operations. Passwords must not be shared with students, other staff

members, substitutes, or the public. Staff members must not log into computers for others to use.

3. Harassment: Use of the District's electronic information, network resources & communications services to transmit information that is discriminatory, harassing or offensive to others, or material that defames an individual, company or business, or discloses personal information without authorization is prohibited.
4. Prohibited Content: Staff are responsible for complying with applicable federal, state, and county laws, regulations, and policies when accessing content or using District network resources, including wireless access. Applicable laws and policies also include those regarding copyright, records retention, privacy laws (FERPA) and information security policies established by DASD. (See U.S. Copyright Office--Fair Use or Copyright Resources.) Use of the District's Electronic Information, Network Resources & Communications Services to access pornographic sites, images, or content is expressly prohibited. See Administrative Regulation 3.8(1) Sexual Harassment. If objectionable material is received or inadvertently accessed, the user should inform his or her supervisor of the incident and close the content.
5. Unlawful Use: Use of the District's Electronic Information, Network Resources & Communications Services and Social Media in violation of any local, state or federal law is prohibited. This includes, but is not limited to, laws and policies regarding pornographic material, gambling, hate speech, copyright, records retention, privacy laws (FERPA), and information security policies established by DASD.
6. Non-Educational Uses: Use of the District's electronic information, network resources, and communications services should not disrupt the educational process. This use includes, but is not limited to, conducting personal business, running a business for commercial or financial gain, soliciting or lobbying for political or religious causes, engaging in unethical or disruptive activities, and sending or forwarding inappropriate messages is prohibited. Accessing the District's electronic information, network resources, and communications services for personal use beyond infrequent and incidental use is prohibited during the work day outside of break or lunch time.
7. Employee Conduct: Appropriate use of District electronic information, network resources, and communications services is a privilege as well as a requirement for effective teaching and learning. Failure to comply with this acceptable use policy's guidelines and rules may result in corrective and/or disciplinary and/or law enforcement action consistent with Board policy, other administrative guidelines, pertinent standards of professionalism and/or law enforcement requirements.

<u>Directory Data</u>

DASD designates the following as directory data: student's name; weight and height of members of athletic teams; photograph, including videotape for educationally related purposes; dates of attendance; degrees, honors (including honor roll) and awards received; and major field of study. This directory data shall be considered public information and may be released to appropriate persons unless parent/guardian of student refuses the release on the "Denial of Release Form - Public Release of Student Information (Directory Data)" form or in writing to the District. "Public" use of directory data includes the above-mentioned applications, and may also include media coverage, District publications (print and web), videotaping/filming, and social media. DASD directory data and web guidelines are to be used when posting student photos, work, links, and information. These documents may be found at the School & Community Relations and Learning Information Systems web pages. More information is available on the Denial of Release Form (Public Release of Student Information - Directory Data) that is available on the District website (Families / Forms).

Device Checkout

Your Responsibilities:

Mobile devices are intended to be used for staff productivity and instruction during the work day. Although incidental personal use is allowed under the District's Acceptable Use Policy, the device's primary use is for District operations and instruction.

- Treat your device as if it were your own.
- Bring your device with you to work each day.
- Report issues immediately.

Your Agreement:

1. The staff member agrees to handle the device carefully and protect it from potential sources of damage or theft. These potential sources might include:
    a. Unlocked or empty classroom
    b. Food and drink
    c. In a vehicle, especially in extreme temperatures
    d. In a vehicle, left in plain sight
2. The device is the property of DASD. If a staff member leaves DASD employment, the device is to be returned immediately to the Learning Information Systems Department (LISD).
3. The staff member must report theft (or suspected theft) of the device, loss of the device, damage to the device to his or her supervisor and LISD immediately.
4. The staff member agrees to follow all DeForest Area School District (DASD) regulations and policies including, but not limited to, the Staff Acceptable Use Policy, as well as all applicable State and Federal laws, including copyright and intellectual property law, pertaining to software and information.
5. The staff member shall not remove or alter any DASD identification labels, tracking software, or the device's name/identification.
6. Any technical issues should be reported via the District's Technology Request system.
7. The staff member agrees to return the equipment before the last official work day or promptly when requested by his or her supervisor or the Learning Information Systems Department (LISD).
8. The device is to be used only by the staff member it is issued to or by a student in the classroom once precautions have been taken to ensure students don't have access to the teacher's email or personal data.