522.6 STAFF INFORMATION & COMMUNICATION TECHNOLOGIES ACCEPTABLE USE POLICY

The School District provides access to communication and information resources to help employees do their job and be well informed. This includes Internet access, the email system, telephones, and all other hardware and software connected to the district's voice, data, or video networks. These resources represent a considerable commitment of financial and human capital for telecommunications, networking, software, storage, etc. The following rules are designed to help everyone use the school district's technology resources wisely. Employees have no expectation of privacy in District provided communication and information resources. The School District has the right to inspect, monitor, or search such resources at any time.

All other school district policies also apply to conduct on the school district's voice, data, and video networks and equipment.

While the district's technological resources offer many potential benefits, including better communication and connections to the world, they also open the door to some significant liabilities. Therefore, each employee is expected to understand and comply with the following rules. Violation of these rules will result in disciplinary action, up to and including termination and/or legal action, if warranted.

Access and Passwords

Network access is granted to individual users to secure information and maintain accountability. Passwords and usernames are how individual access is granted and security is maintained.

1. To preserve security, users should protect passwords and change them periodically. Employees shall not share passwords or post them in public view. If a password is discovered, it will be changed immediately. An employee must immediately report to IT if they believe their password has been discovered by another person.
2. The use of unassigned passwords to gain access to another person's files is prohibited. No one except authorized district support personnel shall use another employee's sign-on protocol (i.e., username and password) without explicit administrative approval.
3. Employees should log off the network when the PC or terminal is not in use.
4. Unauthorized access will be recorded and investigated. Any suspected misuse shall be reported to the IT department.
5. Personal hotspots are prohibited.

Electronic Mail (e-mail)

All email on the school district's networks should be thought of as being written under Williams Bay School District letterhead. Employees should refrain from discussing topics or conveying opinions that they would not put in written form or share with a wider audience. Public record laws generally apply to electronic transmissions in the same manner as they would to paper records. The following rules shall apply:

1. All messages and files created, sent, or received using school district equipment, networks, or email systems are the property of the school district.
2. No employee should have any expectation of privacy with respect to email messages sent through district-provided email accounts. The administration may access and view messages in district provided email for any reason.
3. Please contact the IT department if you receive a virus alert or experience a security breach.
4. E-mail messages (sent, forwarded, or maintained) may not contain content considered offensive or in violation of any applicable board policy. Offensive content includes, but is not limited to, language or images that are (a) libelous; (b) obscene or sexually explicit; (c) harassing (as defined in Policy 512, Employee Harassment); or, (d) discriminatory or potentially creating a hostile environment (for any individuals or groups identified in Policy 511, Equal Opportunity Employment).
5. Employees may not read email that was not sent to them unless officially authorized by their supervising administrator or by the intended email recipient.
6. E-mail messages shall not be used for private business ventures, personal gain, political promotion or campaigning, or any illegal activity. Use of district resources for illegal activity can be cause for termination, consistent with applicable employee handbooks and/or district policy. The district will cooperate with legitimate law enforcement investigations.
7. Users may not send email messages with the sender's identity forged or send email anonymously.

Internet

No employee should have any expectation of privacy as to their Internet usage on district equipment or networks. The District reserves the right to monitor, record, and review usage of all District owned computer resources, whether on-site or off-site. The District may record, and review websites visited, screen content, programs run, files transferred, communications, (including, but not limited to, email, social media, and chat logs) and any other use. Compute equipment, data thereon, school owned accounts, and data stored "in the cloud" are the property of the District and are subject to monitoring and inspection, without warrant, at any time. Anyone who uses district internet to violate board policy, or any law, is subject to discipline up to and including termination and/or legal action, if warranted.

1. The district reserves the right to inspect all files and information stored in any area of the network, including all district issued devices.
2. Illegal or offensive content may not be displayed, archived, stored, printed, distributed, transmitted, edited, or recorded over district networks or using any district equipment. Offensive content includes, but is not limited to, language or images that are (a) libelous; (b) obscene or sexually explicit; (c) harassing (as defined in Policy 512, Employee Harassment); or, (d) discriminatory or potentially creating a hostile environment (for any individuals or groups identified in Policy 511, Equal Opportunity Employment).
3. Employees shall not intentionally visit and/or search for Internet sites that contain or could reasonably be expected to contain any content prohibited in Internet Rule 3 above. If such a site is inadvertently visited, an employee must provide the IT department with a

written description of the time, date, and address of the site, along with a brief explanation of how it was inadvertently visited. The IT department and employee shall keep such written explanation on file as a response when district monitoring identifier the inappropriate visit and requires further explanation.

4. Use of district resources for illegal activity can be cause for discipline up to and including termination. The district will cooperate with legitimate law enforcement investigations.
5. No employee may use the school district equipment, network, or resources to download or distribute pirated or otherwise illegal software or data.
6. No employee may use the school district's equipment, network, or resources to propagate any virus, worm, Trojan horse, or trap-door program code.
7. Employees may download only software with direct school district applications and/or use and must arrange to have such software properly licensed and registered. Downloaded software must be used only under the terms of its license.
8. Employees may not change the default settings of district Internet software related to content advisories, filtering, or storage times for history, cookies, temporary files, or cache.
9. Employees may not add or remove a drive or other hardware storage devices from their assigned district issued device without the authorization of the IT department and Building Principal. Employees are also prohibited from formatting, reformatting, erasing, or restoring a hard drive on their assigned district issued device without the express authorization of the IT department and Building Principal.
10. Employees who permit student access to the Internet accept professional responsibility for supervising the student(s) and for ensuring that they understand and comply with Rules 1 - 10 above.
11. Employees granted Internet access may use assigned resources for occasional personal research (or browsing) during non-duty break times, or outside contracted work hours. Such use must not interfere with district business, congest the network, and all other Internet use rules must be followed.

Telephones (including cellular and fax machines)

1. As with other forms of information technology resources, occasional personal use of telephones during non-duty break times, or outside contracted work hours may be acceptable when no other forms of communication are feasible. Such use must not interfere with district business or incur additional costs to the district.
2. Employees must not use district telephones for private business ventures, personal gain, political promotion or campaigning, or any illegal activity. Use of district telephones for illegal activity can be cause for discipline up to and including termination. The district will cooperate with legitimate law enforcement investigations.
3. Cellular telephones may be provided to employees whose job functions require mobility and immediate accessibility. Cellular telephones should not be used if a conventional telephone is readily available. Employees must reimburse the district for any charges that accrue from unavoidable personal cellular telephone use. Such reimbursement shall be made within the regular billing cycle.
4. Employees shall not fax personal materials without authorization of their supervisor. If such use is permitted, the employee shall reimburse the district for the actual cost of any

long-distance charges plus $1.00 per personal fax.

5. All rules applying to email messages also apply to voice mail messages and faxes distributed or recorded on district telephone equipment or voice networks.
6. The administration is entitled to access and will regularly review district telephone and fax records.

Software

1. Prior to purchase, all software must be tested and approved by district technology staff. Technology Department staff will support only properly licensed and approved district software.
2. Unauthorized software or data will not be supported on any District computing device. District technology staff members may delete unauthorized software and data on desktop computers, servers, or district issued devices.
3. All software must be properly licensed. It is a violation of district policy to install unlicensed software on a district computer.
4. The installation and use of personal software on district issued devices is prohibited unless specifically authorized in writing by a member of the district technology staff.

LEGAL REFERENCE: Wisconsin Statutes, Sections 943.70, 947.0125, 120.12(1)
Children's Internet Protection Act, Neighborhood Children's Internet Protection Act

APPROVED: July 16, 12
REVISED: September 9, 13
October 9, 2017
November 13, 2017
May 24, 2021