With increased concern about identity theft, unwarranted invasion of privacy and the need to protect personally identifiable information, prior to students being directed by staff to use any cloud-based educational software/application, staff must get approval from the Executive Director for Student Achievement and Instructional Technology . The Executive Director for Student Achievement and Instructional Technology will determine if a formal contract is required or if the terms of service are sufficient to address privacy and security requirements, and if parental permission is needed.

Authorized users of the School District's computer resources include members of the Board of Education, administrators, supervisors, faculty, staff, students, parent/guardian and any other person who has been granted access to the School District's computer resources. Unauthorized use is strictly prohibited. By utilizing the School District's computer resources or personally-owned equipment, the user consents to the School District's exercise of its authority and rights as set forth in this Policy with respect to the School District's computer resources , as well as with respect to any information or communication stored or transmitted over the School District's computer resources.

Faculty, staff members, and students (where applicable) may be provided with e-mail accounts and Internet access. Whenever a user ceases being a member of the School District community or if such user is assigned a new position and/or responsibilities, use of the School District's computer resources for which he or she is not authorized in his or her new position or circumstances shall cease and property returned. When a School District employee separates from service from the School District, access to all School District accounts and email is disabled. All School District business being conducted electronically must be performed with a School District account or service. Employees should not use private email accounts. Email used for School District purposes may be subject to FOIL. There is no expectation of privacy when utilizing School District email.

The School District's computer resources, including all telephone and data lines, are the property of the School District. The School District reserves the right to access, view or monitor any information or communication stored on or transmitted over the network, or on or over equipment that has been used to access the School District's network and it may be required by law to allow third parties to do so. Electronic data, e.g., may become evidence in legal proceedings. In addition, others may inadvertently view messages or data as a result of routine systems maintenance and monitoring or misdelivery.

Users must recognize that there is no guarantee of privacy associated with their use of School District computer resources. Users should not expect that e-mail, voice mail or other information created with t

Google Drive or a similar application and even those marked "personal" or "confidential") are private, confidential or secure.

1. All users must not act in ways that invade the privacy of others, are unethical or fail to comply with all legal restrictions regarding the use of electronic data. All users must also recognize and not violate the intellectual property rights of others.

2. All users must maintain the confidentiality of student information in compliance with federal and state law including, but not limited to, FERPA, HIPAA and Education Law, section 2-d.

3. Disclosing and/or gossiping (including but not limited to via e-mail, voice mail, Internet instant messaging, social media, chat rooms or on other types of Web pages) about confidential or proprietary information related to the School District is prohibited.

4. All users must refrain from acts that waste School District computer resources or prevent others from using them. Users will not access, modify or delete others' files or system settings without express permission. Tampering of any kind is strictly forbidden. Deliberate attempts to tamper with, circumvent filtering or access, or degrade the performance of the School District's computer resources or to deprive authorized users of access to or use of such resources are prohibited.

5. Students may not send broadcast e-mail or broadcast voice mail.

6. Users are responsible for both the content and possible effects of their messages on the network. Prohibited activity includes, but is not limited to, creating or propagating viruses, material in any form (text, sound, pictures or video) that reflects adversely on the School District, "chain letters" (which proffer incentives to relay them to others), inappropriate messages (including discriminatory, bullying or harassing material), and billable services.

7. Official email communications must be professional, ethical and meet the standards of other School District publications bearing in mind that the writer is acting as a representative of the School District and in furtherance of the School District's educational mission.

8. Users are prohibited from using personal links and addresses such as blogs, YouTube videos, etc. in School District email unless used in the furtherance of business of the School District as part of the curriculum of the School District.

9. The School District recognizes the value of teacher and professional staff inquiry,

investigation and communication using new technology tools to enhance student learning experiences. The School District also realizes its obligations to teach resp

The School District maintains a “public” wireless network, a “private” wireless network, an “instructional” wireless network and a “hard wired” network. The “hard wired” and “private” wireless networks are limited only to district-owned and managed devices. Any attempt to connect a personal electronic device to either of these networks will be considered a violation of this policy. The “public” wireless network is the sole network that students and faculty may connect to using their personal electronic devices. The School District reserves the right to alter or disable access to the “public” wireless network as it deems necessary without prior notification.

Personal electronic devices that have the ability to offer wireless access to other devices must not be used to provide that functionality to others in any School District building. The ability to connect personal electronic devices to the School District wireless network is a privilege and not a right. When personal electronic devices are used in School District facilities or on the School District wireless network, the School District reserves the right to:

1. make determinations on whether specific uses of the personal electronic device is consistent with this policy;

2. log internet use and monitor storage disk space utilized by such users; and

3. remove or restrict the user’s access to the internet and suspend the right to use the personal electronic device in School District facilities at any time if it is determined that the user is engaged in unauthorized activity or in violation of Board of Education policy.

In addition, when staff members choose to use their own personal electronic devices to perform job-related functions, the following will apply:

1. 2 789.96 re1 0 0 5045004F>3U functionality to otli 11.04 Tf1 0 0 1 72.024 44ay2.66 T6(de)-40(alte)4(s2 0 61

conscretioth

student or staff member will be responsible for the full replacement cost of the device if the loaned device is lost, damaged, stolen or misused.

Individuals must take all reasonable precautions to prevent unauthorized access to accounts or data by others, both inside and outside the School District. Individuals will not leave any devices unattended with confidential information visible. All devices are required to be locked down when an individual steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

Data files and electronic storage areas shall remain School District property, subject to School District control and inspection. The Executive Director for Student Achievement and Instructional Technology or his/her designee may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy.

1. Each user is responsible for the security and integrity of information stored on his or her computer or voice mail system. Computer accounts, passwords, security codes and other types of authorization are assigned to individual users and must not be shared with or used by others. The School District, at its sole discretion, reserves the right to bypass such passwords and to access, view or monitor its systems and all of their contents. By accessing the district's system, the individual consents to the School District's right to do so.

2. Removing School District computer resources from the School District's facilities and/or relocating

made by the Business Office.

5. Employees shall have no expectation of privacy in the use of School District cellular phones. All cellular phone bills for district-issued phones are the property of the School District and will be used as appropriate to investigate the personal use of district-issued cellular phones.
6. School District cellular phones are valuable and should be handled with due care. If loss, theft, or damage to a School District cellular phone results from the known negligence of the employee to whom such phone is assigned, the employee will be required to reimburse the School District for the repair or purchase of replacement equipment.
7. Upon request, district-