

System Administrator Account Acceptable Use (GBEE E 3)

All staff members who have the responsibility of an administrative account must read and agree to this document annually.

Systems, Data and Network Administrators (SDNAs) by the nature of their work, have privileges and responsibilities that other staff members do not have. Without system privileges, SDNAs would not be able to do their jobs. These privileges must be used with the utmost care for Academy District 20's operational systems and respect for others privacy. These guidelines were developed to articulate responsibilities SDNAs have in addition to those outlined in policy GBEE-Appropriate Use of Technology Resources for Staff.

1. Unless part of your job description is to assist in determining a solution to a known issue, you may not deliberately monitor or observe the content of any specific individual's email, network or Internet traffic or traffic logs, or files stored on file servers or computers.
2. Statement of Confidentiality – In the course of your duties, you may accidentally observe personal, sensitive information of our stakeholders or observe inappropriate file content, e-mails, or Internet access. Inappropriate activity is to be reported to the CIO immediately and should be kept in the strictest confidence to protect the privacy of our stakeholders.
3. Performing Tests on the Network – Unless part of your job description and to assist in determining a solution to a known issue, you are not allowed to test the integrity or security of the network to identify flaws. This includes, but is not limited to: security testing, penetration testing, and performance testing and probing or scanning the network. If you are aware of any flaws, they should be communicated immediately to the CIO and kept in confidence.
4. Software Loading/Testing – You are permitted to install approved software on any Academy District 20 computers as part of your job duties. All software on district resources should support the mission of Academy District 20. Documentation and proof of purchase for all site purchased software installed must be approved through the district hardware/software purchasing process prior to purchase and install.
5. SDNAs must not disclose privileged and confidential information about Academy District 20's systems or any other information that could prove detrimental to operations or compromise system security.
6. Use of Encryption - You may only use encryption that is included as part of an operating system package.
7. Possession and Use of Hacking Software - Unless part of your job description and approved by the CIO, possession or use of hacking software is prohibited. Password and file recovery may be performed only as part of your job description. Notify the CIO before the recovery process begins.
8. Each SDNA will take all practical measures to ensure that all hardware and software license agreements are faithfully executed on all systems, networks, servers, and computers for which he or she has responsibility.

Violations of this policy will be handled following the administrative and disciplinary processes outlined in the applicable administrative policies and procedures of the district.

Adopted: July 1, 2015