Title: **Staff Responsible Use of Digital Resources – System Administrator Agreement**
Code: GBEE E 2
Section: Section G: Personnel Policies

All Academy District 20 staff members who have the responsibility of an administrative account must read and agree to this agreement 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 the District's operational systems and respect for the privacy of others. These guidelines were developed to articulate responsibilities and provide exceptions SDNAs have to those outlined in policy GBEE Staff Responsible Use of Digital Resources, to which they would be in violation of when performing SDNA duties.

Unauthorized Use of Access and Non-Disclosure
SDNAs shall not monitor or observe the content of any individual's email, network or Internet traffic or traffic logs, or files stored on file servers or devices unless it is part of their essential job functions or requested by the Chief Information Officer (CIO) or designee. SDNAs shall not disclose privileged and confidential information about the District's systems or any other information that could prove detrimental to operations or compromise system security. If elevated privileges are necessary for problem resolution, SDNAs **must** remove these privileges immediately after the problem has been resolved.

Statement of Confidentiality
In the course of performing SNDA duties any discovered sensitive or personal information shall be kept confidential. Inappropriate activity shall be reported to the CIO or SDNA's Supervisor immediately and kept in the strictest confidence to protect the privacy of the district stakeholders.

Performing Tests on the Network
SDNAs shall not test the integrity or security of the network to identify flaws unless it is part of their essential job functions and requested by the CIO or designee. This includes, but is not limited to: security testing, penetration testing, and performance testing and probing or scanning the network. If an SDNA becomes aware of any flaws, they should keep it confidential and communicated immediately to the CIO or SDNA's Supervisor.

Software Installation
SDNAs are permitted to install software on any District device as part of their essential job functions. All software that collects or stores student Personally Identifiable Information (PII) shall adhere to the provisions of the Colorado Student Data Privacy Act. SDNAs must ensure that all software is appropriately licensed and for which current security patches are available. SDNAs are responsible for applying security patches or uninstalling this software immediately from the network.

Use of Encryption
Only SDNAs may install and use encryption software that is included as part of an operating system package, and intended for keeping district business safe and secure..

Possession and Use of Hacking Software
Possession or use of hacking software is prohibited unless it is part of the SDNAs essential job functions and has been authorized by the CIO. Password and file recovery may be performed only as part of the SDNAs essential job functions. Notify the CIO before the recovery process begins.

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/she has responsibility.

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

Adopted: July 1, 2015
Revised: July 1, 2018
July 1, 2019
January 1, 2022
July 1, 2024
July 27, 2026