

|              |                                                                               |
|--------------|-------------------------------------------------------------------------------|
| Book         | Administrative Policies                                                       |
| Section      | Section G: Personnel Policies                                                 |
| Title        | Staff Responsible Use Agreement of the Internet and Electronic Communications |
| Code         | GBEE E 1                                                                      |
| Status       | Active                                                                        |
| Adopted      | January 1, 2014                                                               |
| Last Revised | July 1, 2022                                                                  |

### **Blocking or Filtering**

To protect students and staff, Academy District 20 utilizes tools that block or filter material and information in accordance with the Children's Internet Protection Act (CIPA) on all digital resources accessing the Internet or electronic communications via Academy District 20 networks.

### **No Expectation of Privacy**

Staff members shall have no expectation of privacy when using the Internet, digital resources, or electronic communications. The District reserves the right, at any time and without prior notice, to monitor, inspect, copy, log, and review activity on the District network and digital resources. All material and information accessed/received through District digital resources shall remain the property of Academy District 20 and may be subject to disclosure under the Colorado Open Records Act (CORA).

### **Inappropriate Use**

The use of Academy District 20 property and Information Technology Services is a privilege and not a right. Inappropriate use or vandalism may result in disciplinary measures, including loss of digital resource and network privileges, suspension, or civil or criminal liability under applicable laws. An account may be suspended at any time should inappropriate activity occur, or if directed by school or district administration. Because technology and ways of using technology are constantly evolving, not every unacceptable use of district digital resources can be specifically described in policy. Examples of unacceptable uses include, but are not limited to, the following:

- publish, access, download, store, review, and/or distribute any content (text, graphic, photo, audio) that contains material, which is defamatory, abusive, obscene, profane, threatening, or sexually explicit
- harass, threaten, intimidate, bully, demean, or promote violence or hatred against another person or group of persons with regard to disability, race, creed, color, sex, sexual orientation, marital status, national origin, religion, ancestry, age, genetic information, or conditions related to pregnancy or childbirth
- use District resources and/or the District network for personal profit, financial gain, or advertising;
- use District resources for political campaign activities in violation of the Colorado Fair Campaign Practices Act (C.R.S. 1-45-101, et seq.)
- publish information that is knowingly false or could be construed as intending to purposely damage another person's reputation
- violate any federal or state law, or district policy, including but not limited to, copyrighted material and material protected by trade secret
- use information protected by applicable privacy and confidentiality laws
- use another individual's Internet or electronic communications account
- impersonate another individual or transmit through an anonymous manner
- use or attempt to use an Internet proxy server (anonymizer), proxy software, or proxy browser

- configure any device to provide unfiltered Internet access for yourself or other user(s)
- perform tests on the District network to identify security faults
- use non-district encryption to cloak network traffic, data files, or email communications within the District network
- possess, install or use malicious software, hacking software, proxy software, or devices used for these purposes on District property, including, but not limited to capturing software or devices, network discovery and monitoring software or devices, password recovery software and devices, and software specifically designed to remove the evidence of user activity from a computer.

### **Accounts, Passwords, and Security**

In order to access District resources outside of the District network, staff is required to register for Multi-Factor Authentication (MFA). Staff should maintain a strong password that is complex in nature and not easily guessed. Malware and Phishing are increasingly frequent and more complex. Staff members should use extreme caution when opening emails and/or attachments or clicking on links within them. It is the responsibility of the staff member to report any suspicious emails and/or attachments to the District's Help Desk. Staff members should not demonstrate the problem to other users.

### **Staff shall not:**

- use another person's login or password even if permission from the other person is granted;
- share login credentials with anyone, including supervisors, IT, Help Desk, co-workers, secretaries, substitutes, etc.
- record and store their login credentials on or near their computer (i.e. post-it notes on the monitor, desk, etc.)
- store student or District confidential data on a non-District device or system, including personal cell phones, tablets, laptops, and cloud storage, install encryption software or encrypt a District-owned device
- leave a District-owned or personally owned digital resource unattended while logged in, or allow any other person to use that device while logged in
- store email in a local PST file
- gain unauthorized access to the District network, servers, or District-owned systems.

Any staff member identified as a security risk, intentionally violating, or having a history of violating District policy regarding digital resources may have their access revoked to District resources and may be subject to disciplinary action up to and including dismissal from employment. When a staff member leaves the District, it is his/her responsibility to move their data from District-supported online productivity suites (0365 and Google) prior to their last day, or data will be lost.

### **Confidentiality and Privacy**

Staff members shall not access, transmit, or forward material that is protected by confidentiality laws unless such access is in accordance with their assigned job responsibilities, and applicable law and District policy. Staff members shall handle all personnel, student, and District records in accordance with policies GBJ (Personnel Records and Files) and JRA/JRC. Staff members who share confidential student information via electronic communications shall utilize encryption tools through Microsoft 0365, so that confidential records are not inadvertently sent or forwarded to the wrong party. Staff members shall include the email confidentiality notice on their email signature on any digital resources that send email. The notice should state the following:

**Confidentiality Statement:** *This email message contains information from Academy District 20. The information contained in this email may be confidential and is intended only for the use of the recipient named above. If you are not the intended recipient, please delete the original message without disclosing, distributing, or copying. Under the Colorado Open Records Act (CORA), all messages on this district owned e-mail account may be subject to public disclosure.*

### **Use of Social Media**

Social media refers to interaction in which people create, share, and/or exchange information and ideas in a virtual or online environment. Staff shall not interact with currently enrolled students with their personal online account and must not accept invitations from current students. Staff members will utilize only District supported platforms in lieu of social media for instructional purposes and/or other school-related matters, including

promoting communications with students and parents/guardians. As with any other instructional material, the application/platform and content shall be appropriate to the student's age, understanding, and range of knowledge.

Staff members are expected to serve as positive role models and represent their school and District professionally at all times. All off-campus expression on social media that is made pursuant to a staff member's official job duties is subject to this policy.

Staff members are expected to protect the health, safety, and emotional well-being of students and to preserve the integrity of the learning environment. Online or electronic conduct that distracts or disrupts the learning environment or other conduct in violation of this or related District policies may form the basis for disciplinary action up to and including dismissal from employment.

### **Vandalism**

Vandalism will result in the cancellation of privileges and may result in school disciplinary action and/or legal action. Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse, or disrupt the operation of any network or system within the school district.

### **Unauthorized Software**

Staff members are prohibited from installing any software that has been personally purchased. Additionally, unauthorized software includes, but is not limited to, the uploading or creation of computer viruses, malware, the use of third-party encryption software, and personal virtual private networks (VPNs).

### **Staff Member Use is a Privilege**

Use of the Internet and electronic communications demands personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Staff members' use of the Internet and electronic communications is a privilege, not a right. Failure to follow the use procedures contained in this policy shall result in the loss of the privilege to use these tools, restitution for costs associated with damages, and may result in disciplinary action up to and including dismissal from employment and/or legal action. The school District may deny, revoke, or suspend access to District digital resources or close accounts due to violations of this policy.

Staff members shall be required to electronically sign and agree to this policy annually before Internet or electronic communications accounts shall be issued or access shall be allowed.

### **School District Makes No Warranties**

The District makes no warranties of any kind, whether expressed or implied, related to the use of District computers and computer systems, including access to the Internet and electronic communications services. Providing access to these services does not imply endorsement by the District of the content, nor does the District make any guarantee as to the accuracy or quality of information received. The District shall not be responsible for any damages, losses, or costs a staff member suffers in using the Internet and electronic communications. This includes loss of data and service interruptions. Use of any information obtained via the Internet and electronic communications is at the staff member's own risk.

**Adopted:** January 1, 2014

**Revised:** July 1, 2014

July 1, 2015

July 1, 2016

July 1, 2018

July 1, 2019

July 1, 2020

July 1, 2021

July 1, 2022