## Section G: Personnel

## GCSA-R Employee Digital Device and Internet Use Rules

Each employee is responsible for their actions and activities involving school digital devices, printers, networks, internet services and other technology, and for their computer files, passwords and accounts. These rules provide general guidance concerning the use of the school's digital devices and examples of prohibited uses. The rules do not attempt to describe every possible allowed or prohibited activity by employees. Employees who have questions about whether a particular activity or use is prohibited are encouraged to contact a building administrator or the Technology Director.

### A. Access to School Digital Devices and Acceptable Use

The level of employee access to school digital devices, network, and internet services is based upon specific job requirements and needs. Unauthorized access to secure areas of the school's digital devices, internet and networks is strictly prohibited.

All Board policies, school rules and expectations for professional conduct and communications with others including other staff, students and parents apply when employees are using the school's digital devices, printers, network and internet services, whether in use at school or off school premises.

### B. Prohibited Uses

Examples of unacceptable uses which are expressly prohibited include, but are not limited to, the following:

1. Any use that is illegal or which violates Policy GCSA and/or other Board policies, procedures or school rules, including harassing, discriminatory or threatening communications and behavior; violations of copyright laws or software licenses. Region 8 assumes no responsibility for illegal activities of employees while using school digital devices, network infrastructure and/or internet service.

2. Any attempt to access unauthorized web sites, apps, or any attempt to disable or circumvent the school's filtering/blocking technology.

3. Any use involving materials that are obscene, pornographic, sexually explicit or sexually suggestive, or harmful to minors.

4. Any communications with students or minors for non-school-related purposes.

5. Downloading “apps” or using or encouraging students to use other online educational services without prior authorization from the Director or the Technology Director.

6. Any use for private financial gain, commercial, advertising or solicitation purposes.

7. Any sending of e-mail or other messages to groups of school employees (except in the performance of their duties as school employees) without authorization from the Director/designee. Prohibited uses of the school’s message systems also include but are not necessarily limited to:

    a. Solicitation of membership in any non-school-sponsored organizations or associations
    b. Advocacy or expression by or on behalf of individuals or non-school-sponsored organizations or associations
    c. Political or religious purposes
    d. Raising funds for non-school-sponsored purposes, whether profit-making or not-for-profit
    e. Selling articles or services of any kind, advertising or promoting any kind of business, or
    f. Any communications that represent an employee’s views as those of Region 8 or that could be misinterpreted as such

8. Sending mass e-mails (SPAM) to school users or outside parties for any purpose without the permission of the Director.

9. Sharing passwords or other login information (except with authorized school employees), using other users’ passwords and/or login information, accessing or using other users’ accounts; or attempting to circumvent network security systems.

10. Any malicious use, damage or disruption of the school’s digital devices, printers, network, internet services or other technology; any breach of security features; any failure to report a security breach; or misuse of passwords or accounts (the employee’s or those of other users).

11. Any attempt to delete, erase or otherwise conceal any information stored on a school digital device that violates these rules or other Board policies or school rules, or refusing to return digital devices or equipment issued to the employee upon request.

## C. Disclosure of Confidential Information

Employees are expected to use appropriate judgment and caution in communications concerning students and staff to ensure that personally identifiable information remains confidential.

E-mail, apps and other internet communications mechanisms (including web sites, blogs and social networking sites) should not be considered secure or private. Communications with students or minors via e-mail or other digital means must be for school related educational purposes only. Private use of social networking or other sites with students or other minors is strongly discouraged.

## D. Employee/Volunteer Responsibility to Supervise Student Digital Device Use

Employees and volunteers who use school digital devices with students for instructional purposes have a duty of care to supervise such use and to enforce the school's policies and rules concerning student digital device use. When, in the course of their duties, employees or volunteers become aware of a student violation, they are expected to stop the activity and inform the Director or a building administrator.

## E. Compensation for Losses, Costs and/or Damages

The employee is responsible for compensating the school for any losses, costs or damages incurred by the school for violations of Board policies and school rules while the employee is using school digital devices, including the cost of investigating such violations. The school assumes no responsibility for any unauthorized charges or costs incurred by an employee while using school digital devices.

Any damage or theft to school property must be reported immediately to the Director and/or the Technology Director.

## F. Additional Rules for Use of Privately-Owned Digital Device by Employee

1. An employee who wishes to use a privately-owned computing or printing device in school must notify the Director and Technology Director. There must be a legitimate work-related basis for any request.

2. The Technology Director will determine whether an employee's privately-owned digital device meets the school's network requirements.

3. Requests may be denied if it is determined that there is not a suitable work-related reason for the request and/or if the demands on the school's network or staff would be unreasonable.

4. The employee is responsible for proper care of their privately-owned digital device, including any costs of repair, replacement or any modifications needed to use the digital device at school.

5. The school is not responsible for damage, loss or theft of any privately-owned digital device.

6. Employees are required to comply with all Board policies, administrative procedures and school rules while using privately-owned digital devices at school.

7. Employees have no expectation of privacy in their use of a privately-owned digital device while it is being used at school. The contents of the digital device may be searched in accordance with applicable laws and policies.

8. The school may temporarily confiscate any privately-owned digital device brought to school and used by an employee in school without authorization as required by these rules.

Cross Reference: GCSA – Employee Digital Device and Internet Use
EGAD – Copyright Compliance

First Reading: 4/27/11, 6/27/18, 9/22/21, 10/23/24
Adopted: 5/25/11, 8/22/18, 10/27/21, 11/20/24
Revised: 10/15/24
Reviewed: 5/23/18