ACCEPTABLE USE OF TECHNOLOGY POLICY

The Collaborative Charter Services Organization ("SOCS" or the "CSO") recognizes that technological resources enhance employee performance by offering effective tools to assist in providing a quality instructional program; facilitating communications with parents/guardians, students, and the community; supporting CSO operations; and improving access to and exchange of information. The CSO expects all employees to learn to use the available technological resources that will assist them in the performance of their job duties and will provide professional development as needed in the appropriate use of these resources.

The CSO permits employees to use its technology and communication systems, including email, phones, voicemail, digital CSO programs, and internet, subject to the following:

1. The technology and communication systems provided by the CSO are the property of the CSO. All electronic communications, including all emails, software, databases, hardware, and digital files, remain the sole property of the CSO and are to be used only for CSO business. Employees have no reasonable expectation of privacy in their use of such technology and communications.

2. The CSO may periodically assign and/or change passwords and personal codes for voice mail, email and computer. The CSO reserves the right to override any such password system at any time at its sole discretion, with or without cause.

3. The CSO will allow some minimal personal use by employees if such use does not disrupt or interfere with the employee's timely performance of job duties and is consistent with law and CSO policy. The following exceptions remain in place:
    a. The CSO reserves the right to require authorization prior to the installation of software on a CSO computer and/or mobile devices.
    b. With CSO approval, employees may use personal passwords for purposes of security, but any employee's use of a personal password does not affect the CSO's ownership of the electronic information.
    c. All electronic information created by any employee using any means of electronic communication is the property of the CSO and remains the property of the CSO.

4. CSO technology and communication systems are not to be used in any way that may be disruptive, offensive, harmful to morale, engages in copyright or trademark infringement, and otherwise violates the law or CSO policy. For example, sexually explicit images, ethnic slurs, racial epithets, or anything else that may be construed as harassment or disparagement of others based on race, national origin, sex, sexual orientation, age, religious beliefs or political beliefs may not be displayed or transmitted.

Employees must not attempt to gain access to another employee's or third parties' personal files, email, or voicemail without express permission given. As the technology and communication systems are the property of the CSO, it will retain a copy of all employee-used passwords. Employees may not use passwords or security measures unknown to the CSO. System security

features, including passwords and delete functions, do not neutralize the CSO's ability to access any digital records at any time. Employees must be aware that the possibility of such access always exists. The CSO reserves the right to access and review electronic files, messages, mail, and other digital archives, and to monitor the use of electronic communications as necessary to ensure that no misuse or violation of CSO policy or any law occurs.

5. Employees who use their personal phones, voicemail,, and text messages for School-related communications, may be subject to disclosure under the Public Records Act. It is recommended that school-related communications take place using school-issued communications and technology systems when possible. All school-related email communications must be sent using the employee's school email account.

6. Access to the Internet, websites, and other types of CSO-paid computer access are to be used for CSO related business. Any information about the CSO, its products or services, or other types of information that will appear in the electronic media about the CSO must be approved by the CEO or designee before the information is placed on an electronic information resource that is accessible to others.

7. Employees shall report any security problem or misuse of CSO technology to the CEO, CSO director, or designee.

Social Media

The CSO supports the use of social media and online platforms (including websites, blogs, and forums) by staff members to assist in their professional duties and to create an online presence that facilitates staff, parent/guardian, students, and community communication. All communications with staff and students through social media, or other online platform, should be limited to matters directly related to the employee's professional duties. Staff must exercise good judgment and maintain professional standards and boundaries when interacting with students both on and off CSO property, including through digital communication. Use of social media for personal use during CSO time or on CSO equipment is prohibited.

Employees must avoid posting any information or engaging in communications that violate state or federal laws or CSO policies.Employees must make clear that any views expressed are the employee's alone and do not necessarily reflect the views of the CSO. Employees may not act as a spokesperson for the CSO or post comments as a representative of the CSO, except as authorized by the CEO, CSO director, or designee. When authorized as a spokesperson for the CSO, employees must disclose their employment relationship with the CSO. The use of the CSO logo(s) on a social media site or elsewhere must be pre-approved by the CEO, CSO director, or designee.

Any employee who is found to have neglected or misused the CSO's property will be subject to disciplinary action up to and including termination. If an employee's misuse of the CSO's property damages the property, the CSO reserves the right to require the employee to pay all or part of the cost to repair or replace the property. Misappropriation of the CSO's property is

grounds for immediate termination and possible criminal action. Inappropriate use of CSO technology may result in cancellation of the employee's user privileges, disciplinary action, and/or legal action in accordance with law.

Upon employment and whenever significant changes are made to the CSO's policy, employees shall be required to acknowledge that they have read and agree to the policy.