Type:	School Operations
Title:	**Technology Usage Policy**
Date of Board Approval:	June 2020
Notes:	

Section 1. Purpose

City Garden Montessori School's (CGMS) technology exists for the purpose of enhancing the educational opportunities and achievement of CGMS students. In addition, technology assists with the professional enrichment of the staff and increases engagement of students' families and other CGMS patrons, all of which positively impact student achievement. The purpose of this policy is to facilitate access to CGMS technology and to create a safe environment in which to use that technology.

Section 2. Definitions

For the purposes of this policy and related procedures and forms, the following terms are defined:

Section 2.1 Technology Resources – Technologies, devices and services used to access, process, store or communicate information. This definition includes, but is not limited to: computers; modems; printers; scanners; fax machines and transmissions; telephonic equipment; mobile phones; audio-visual equipment; Internet; electronic mail (e-mail); electronic communications devices and services, including wireless access; multi-media resources; hardware; and software. Technology resources may include technologies, devices and services provided to the school by a third party.

Section 2.2 User – Any person who is permitted by CGMS to utilize any portion of CGMS's technology resources including, but not limited to, students, employees, Board members and agents of CGMS.

Section 2.3 User Identification (ID) – Any identifier that would allow a user access to CGMS's technology resources or to any program including, but not limited to, e-mail and Internet access.

Section 2.4 Password – A unique word, phrase or combination of alphabetic, numeric and non-alphanumeric characters used to authenticate a user ID as belonging to a user.

Section 3. Authorized Users

Section 3.1 CGMS's technology resources may be used by authorized students, employees, Board members and other persons approved by the Chief Executive Officer or designee, such as consultants, legal counsel and independent contractors. All users must agree to follow CGMS's policies and procedures and sign or electronically consent to CGMS's User Agreement prior to accessing or using CGMS technology resources, unless excused by the Chief Executive Officer or designee.

Section 3.2 Use of CGMS's technology resources is a privilege, not a right. No potential user will be given an ID, password or other access to CGMS technology if they are considered a security risk by the Chief Executive Officer or designee.

Section 4. User Privacy

Section 4.1 A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving CGMS's technology resources including, but not limited to, voice mail, telecommunications, e-mail and access to the Internet or network drives. By using CGMS's network and technology resources, all users are consenting to having their electronic communications and all other use monitored by CGMS. A user ID with e-mail access will only be provided to authorized users on condition that the user consents to interception of or access to all communications accessed, sent, received or stored using CGMS technology.

Section 4.2 Electronic communications, downloaded material and all data stored on CGMS's technology resources, including files deleted from a user's account, may be intercepted, accessed, monitored or searched by the Chief Executive Officer or designee at any time in the regular course of business. Such access may include, but is not limited to, verifying that users are complying with CGMS policies and rules and investigating potential misconduct. Any such search, access or interception shall comply with all applicable laws. Users are required to return CGMS technology resources to CGMS upon demand including, but not limited to, mobile phones, laptops and tablets.

Section 5. Technology Administration

Section 5.1 The Board directs the Chief Executive Officer to assign trained personnel to maintain CGMS's technology in a manner that will protect CGMS from liability and will protect confidential student and employee information retained on or accessible through CGMS technology resources.

Section 5.2 Administrators of CGMS technology resources may suspend access to and/or availability of CGMS's technology resources to diagnose and investigate network problems or potential violations of the law or CGMS policies and procedures. All CGMS technology resources are considered CGMS property. CGMS may remove, change or exchange hardware or other technology between buildings, classrooms or users at any time without prior notice. Authorized CGMS personnel may install or remove programs or information, install equipment, upgrade any system or enter any system at any time.

Section 6. Content Filtering and Monitoring

Section 6.1 CGMS will monitor the online activities of minors and operate a technology protection measure ("content filter") on the network and all CGMS technology with Internet access, as required by law. In accordance with law, the content filter will be used to protect against access to visual depictions that are obscene or harmful to minors or are child pornography. Content filters are not foolproof, and CGMS cannot guarantee that users will never be able to access offensive materials using CGMS equipment. Evading or disabling, or attempting to evade or disable, a content filter installed by CGMS is prohibited.

Section 6.2 The Chief Executive Officer, or designee, or a CGMS technology administrator may fully or partially disable CGMS's content filter to enable access for an adult for bona fide research or other lawful purposes. In making decisions to fully or partially disable CGMS's content filter, the administrator shall consider whether the use will serve a legitimate educational purpose or otherwise benefit CGMS.

Section 7. Online Safety, Security and Confidentiality

Section 7.1 In addition to the use of a content filter, CGMS will take measures to prevent minors from using CGMS technology to access inappropriate matter or materials harmful to minors on the Internet. Such measures shall include, but are not limited to, supervising and monitoring student technology use, careful planning when using technology in the curriculum, and instruction on appropriate materials. The Chief Executive Officer or designee and/or a CGMS technology administrator will develop procedures to provide users guidance on which materials and uses are inappropriate, including network etiquette guidelines.

Section 7.2 All minor students will be instructed on safety and security issues, including instruction on the dangers of sharing personal information about themselves or others when using e-mail, social media, chat rooms or other forms of direct electronic communication. Instruction will also address cyberbullying awareness and response and appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms. This instruction will occur in CGMS's courses that use the Internet in instruction. Students are required to follow all CGMS rules when using school technology resources and are prohibited from sharing personal information online unless authorized by CGMS.

Section 7.3 All CGMS employees must abide by state and federal law and Board policies and procedures when using school technology resources to communicate information about personally identifiable students to prevent unlawful disclosure of student information or records.

Section 7.4 All users are prohibited from using CGMS technology to gain unauthorized access to a technology system or information; connect to other systems in evasion of the physical limitations of the remote system; copy CGMS

files without authorization; interfere with the ability of others to utilize technology; secure a higher level of privilege without authorization; introduce computer viruses, hacking tools, or other disruptive/destructive programs onto CGMS technology; or evade or disable a content filter.

Section 8. Records Retention

Section 8.1 Trained personnel shall establish a retention schedule for the regular archiving or deletion of data stored on CGMS technology resources.

Section 8.2 In the case of pending or threatened litigation, CGMS's attorney will issue a litigation hold directive to the Chief Executive Officer. The litigation hold directive will override any records retention schedule that may have otherwise called for the transfer, disposal or destruction of relevant documents until the hold has been lifted by CGMS's attorney. E-mail and other technology accounts of separated employees that have been placed on a litigation hold will be maintained by CGMS's Chief Operating Officer or designee until the hold is released. No employee who has been so notified of a litigation hold may alter or delete any electronic record that falls within the scope of the hold. Violation of the hold may subject the individual to disciplinary actions, up to and including termination of employment, as well as personal liability for civil and/or criminal sanctions by the courts or law enforcement agencies.

Section 9. Violations of Technology Usage Policies and Procedures

Section 9.1 Use of technology resources in a disruptive, inappropriate or illegal manner impairs CGMS's mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal responsibility is expected of all users granted access to CGMS's technology resources. Any violation of CGMS policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. User privileges may be suspended pending investigation into the use of CGMS's technology resources.

Section 9.2 Employees may be disciplined or terminated, and students suspended or expelled, for violating CGMS's technology policies and procedures. Any attempted violation of CGMS's technology policies or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation. CGMS will cooperate with law enforcement in investigating any unlawful use of CGMS's technology resources.

Section 10. Damages

Section 10.1 All damages incurred by CGMS due to a user's intentional or negligent misuse of CGMS's technology resources, including loss of property and staff time, will be charged to the user. CGMS administrators have the authority to sign any criminal complaint regarding damage to school technology.

Section 11. No Warranty/No Endorsement

Section 11.1 CGMS makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides. CGMS's technology resources are available on an "as is, as available" basis.

Section 11.2 CGMS is not responsible for loss of data, delays, nondeliveries, misdeliveries or service interruptions. CGMS does not endorse the content nor guarantee the accuracy or quality of information obtained using CGMS's technology resources.

Legal Citations

State:

RSMo. 569.095, .099	Computer Data and Computer User Tampering
RSMo. 610.010-.030	Missouri Sunshine Law
RSMo. 182.817	Disclosure of Library Records
RSMo. 431.055	Contract Age of Competency
RSMo. 537.525	Civil Remedies for Computer Tampering
RSMo. 542.404	Wire Communications
Chapter 109, RSMo.	Public and Business Records
Chapter 573, RSMo.	Pornography and Related Offenses

Federal:

18 U.S.C. 2701-2711	Stored Communications Act
18 U.S.C. 2510-2520	Electronic Communications Privacy Act
20 U.S.C. 1232g	Family Educational Rights and Privacy Act
20 U.S.C. 6312	Elementary and Secondary Education Act
47 C.F.R. 54.520	Federal Regulation
47 C.F.R. 54.501-.513	E-Rate
47 U.S.C. 254(h)	Child Internet Protection Act