STEM SCHOOL HIGHLANDS RANCH POLICY
Information Technology and Student Data Privacy

I. PURPOSE

To support its educational mission, STEM School Highlands Ranch (STEM) may provide information technology (IT), such as computers, networks, Internet access, and email accounts, to its students. The STEM Board believes that IT should be used at STEM as a learning resource to educate and to inform, and that STEM has an obligation to teach its students to be responsible IT users.

Subject to this policy, STEM staff shall be free to select and implement IT which STEM, deems best furthers the STEM mission.

While parents and students themselves are ultimately responsible for student behavior at school and student use of STEM IT, STEM will make every reasonable effort to ensure that students use STEM IT appropriately and responsibly. To this end, STEM has implemented content filtering measures that direct student learning and restrict student access to inappropriate material, in accordance with applicable law.

Administrators, teachers, and staff have a professional responsibility to work together and with parents to help students develop the intellectual skills needed to evaluate and choose information sources, to identify information appropriate to the age and developmental levels of the students, and to evaluate and use information to meet their educational goals.

Because all STEM IT is owned, leased, or licensed by STEM, STEM is responsible for all content stored or retained on any STEM-owned IT device or on the STEM's networks (together referred to as "STEM IT activity"). STEM therefore has the right to monitor all School IT activity and students have a limited expectation of privacy in any information they access, receive, or create using or on STEM IT.

STEM IT may periodically fail or be interrupted, leading to loss of data or service interruption, and the School therefore makes no warranties of any kind related to its IT.

STEM shall develop and maintain operational policies addressing
(1) monitoring and tracking of school-issued and student-owned computers;
(2) student use, rights and responsibilities relating to computers used at STEM;
(3) an "instructional technology" policy regarding use of technology in learning, including integrating technology for collaborative purposes, consistent with the STEM mission; and
(4) the training of STEM staff with respect to student laptops and privacy, and the administration, oversight, and enforcement of such policies and regulations.

II. POLICY

The STEM Board authorizes the Executive Director to develop rules and procedures ("Administrative IT Policies") for staff and student use of technology which are consistent with this policy and the following standards.
1. All Administrative IT Policies shall comply with this policy.
2. Before adoption of monitoring software of any nature, STEM shall specifically identify the need for such software and whether there are less intrusive alternatives that can accomplish the same goal or need.
3. Student generated computer data ("SGCD") is data generated by a student while using a computer. Information or data contained on any such computer is "personal computer data" or "PCD". PCD includes specific "user logging information" ("ULI"). "Logging" is the process by which a system collects data about a computer network and the individuals using the network. STEM shall treat both SGCD and PCD as "records" as defined by the Family Educational Rights and Privacy Act ("FERPA").
4. Software that has the ability to collect PCD or SGCD shall not be used or implemented prior to the adoption of Administrative IT Policies governing use of such software.
5. STEM shall obtain informed consent from each student's parent or guardian prior to the installation of any software on any student-owned computer and prior to implementation of any technology which has the ability to collect or monitor PCD, so that prior to the giving of such consent students and their families are fully informed of the ability of any such software or technology to collect and monitor such data and to protect such data.
6. Any technology which permits viewing or collecting of PCD shall not permit such monitoring or collection beyond any legitimate educational interests.
7. Keystroke monitoring technology shall not be used or implemented in the absence of a specific legitimate educational purpose which cannot be achieved without this technology and without specific consent from each student's parent or guardian.
8. STEM shall not log or access PCD or SGCD other than for legitimate educational purposes. STEM shall maintain a record or log of all access or logging which records each instance of access, the data accessed, the identity of the accessing party, and the legitimate educational purpose for such access.
9. The exceptions allowing STEM staff to access PCD, other than where consent is given, shall be limited to situations where there is a reasonable suspicion of violation of either a law or school policy.
10. STEM staff shall complete training regarding technology and technology policies prior to use or implementation of any such technologies.
11. For students (a) who are unable or unwilling to bring personal computers to STEM or (b) whose parent or guardian do not consent to the use or installation of monitoring software on a personal computer, STEM shall use its best efforts to make necessary accommodations to ensure that such student's education is not adversely affected.
12. For computers issued by STEM, students and their parents shall be required to sign acceptable use agreements, which will detail appropriate and inappropriate use of STEM-owned computers.

13. Remote monitoring of any kind, including activation of webcams, screen shots, audio, and video, shall be prohibited.
14. All procedures shall comply with applicable state and federal law.
B. In addition to rules specifically concerning IT, general policies, regulations, and rules governing student conduct apply to the use of IT. Violating such policies, regulations, or rules may result in the loss of the privilege to use some or all of the School's IT, discipline (which can include suspension and expulsion), reimbursement to the School for unauthorized charges or costs, civil legal proceedings, and referral to law enforcement authorities. The School may provide examples of prohibited uses of IT in handbooks or Administrative IT Policies.

Sources:
20 U.S.C. 1232, Family Educational Rights and Privacy Act
47 U.S.C. 201 et seq., Communications Decency Act of 1995
47 U.S.C. 231 et seq., Children's Online Privacy Protection Act of 2000
C.R.S. 22-87-101 et seq., Children's Internet Protection Act
DCSD Policy JICD, Student Use of District Information Technology

Approved by the STEM School Board on __11/10/2022__.
(dd/mm/yyyy)
STEM School Highlands Ranch

By: _____*Michelle Horne*__(*signature on file)*_____
(Signature, Board secretary)

_____Michelle Horne_____
(Printed name, Board secretary)

Adopted: 2013
Revised: October 2022