USE OF TECHNOLOGY RESOURCES BY STUDENTS

Code **IJNDB-R2** *Issued* **4/19**

Fort Mill School District (FMSD) provides students with access to variety of technological and electronic resources to support and enhance the academic, social, and emotional achievement of students in the district. Risks exist in the use of these resources, which require the cooperation of student users as a component of that risk management. This administrative rule is established in alignment with district policies EHA, *Data and Internet Security*, IJNDB, *Acceptable Use of Technology Resources*, and the district information security program. This rule is intended to ensure the safety and privacy of our students, to protect data and our resources, and to safeguard the overall integrity of both the FMSD and its students. We request that parents/legal guardians and students familiarize themselves with this rule as outlined below.

Primacy of Instructional Delivery Statement

Given the integration of online and networked content into the delivery of the curriculum in many classes, responsible use of electronic resources by students is essential to the program of education. Unacceptable use by a student may result in enhanced supervision, reduced or revoked access to specific resources, alternative delivery of content, probationary measures, re-instruction in acceptable use, and/or other measures designed to mitigate adverse educational consequences. However, this does not prevent other disciplinary responses.

The following rules and procedures apply to all students enrolled in district schools on and off campus.

The district gives the following notices and retains the following rights:

- To log network use.
- To remove a user account on the network.
- To monitor students' online activities and the use of district-owned devices. This may include real-time monitoring of network activity and/or maintaining a log of Internet activity for later review.
- To provide internal and external controls as appropriate and feasible. Such controls will include the right to determine who will have access to district-owned equipment and, specifically, to exclude those who do not abide by the acceptable use policy or other policies governing the use of school facilities, equipment, and materials. The district reserves the right to restrict online destinations through software or other means.
- Users should not have any expectation of privacy in any information accessed, viewed, downloaded, stored, transmitted, or received using the district's network resources or in the contents or use of district-owned devices.
- The district will not be liable for students' inappropriate use of the district's electronic communication resources or violations of copyright restrictions, students' mistakes or negligence, or costs incurred by students.
- The district will not be responsible for ensuring the accuracy or usability of any information found on the Internet.

 (see next page)

- The district uses technology protection measures to protect students from inappropriate access, but no such system is perfect. It is not possible to constantly monitor each individual student in his or her use the network.

- The district has security measures in place; however, such measures do not guarantee total security. As a result, information generally considered to be personal or confidential should not be sent via the district's communication resources except through means deployed for that purpose or approved for that purpose. The district does not assume responsibility for lost or stolen information sent or received via the district's communication resources.

- Pursuant to the Electronic Communications Privacy Act of 1986 (18 U.S.C 2510, *et seq*.), notice is hereby given that there are no facilities provided by this system for sending or receiving private or confidential electronic communications.

- The district will not be responsible for any damages you may suffer, including loss of data resulting from delays, non-deliveries, or service interruptions. Use of any information obtained is at your own risk.

- An Information Security Program is in place in the district. Generally, a student's role under that program is to be a responsible user. However, during incident responses or for other purposes of the program, specific directions from the administrators of that program from must be observed by all users.

- The district reserves the right to change its policies and rules at any time.

User responsibilities for acceptable use

- The guiding principle for investing district resources in information technology provided to students is that all use of those resources must be in support of educational and research objectives consistent with the mission and objectives of the district.

- Students will receive instruction on proper use of district-owned devices and the district's network and internet system, including e-mail accounts (when provided), in the specific settings applicable to the academic program and purposes for which the resources are being made available to that student. Students must comply with these instructions.

- District owned devices are there responsibility of the students to whom they are issued, both with respect to loss or damage of the device and with respect to the misuse of the device. Accordingly, students should take measures to limit access by others to their district-issued devices, including but not limited to safeguarding usernames and passwords.

- Where a user suspects that any element (accounts, webpages, software, data, etc.) of the district's information technology has been, or is, damaged, threatened, or compromised by hacking, virus, data breach, or the like, the incident must be reported promptly to the student's teacher or building administration in order to implement an incident response under the district's information security program.

Examples of unacceptable use

The following is not an exhaustive list of unacceptable uses under the general requirements stated above.

- using information technology to facilitate violating other school rules and policies, including discipline code violations

 (see next page)

- using information technology to create or disseminate content reasonably perceived as threatening, bullying, obscene, sexual, racist, or otherwise discriminatory
- using information technology in ways that violate copyrighted/intellectual property of others
- using information technology for unlawful purposes
- using information technology for commercial or for-profit purposes
- misrepresenting other users on the network
- circumventing or disabling security measures in place under the information security policy
- installing unauthorized hardware or software
- purposefully accessing material, including material inappropriate for minors, intended to be excluded from the district system under the district's program of technology protection measures, even if the technology protection measures fail to block it

Students who witness, experience, or otherwise learn about a suspected violation are required to report the matter to a teacher or administrator.

Issued 4/9/19