Book	District Policies - Jefferson County School District R-1
Section	J: Students
Title	Student Use of Personal Devices
Number	JSA
Status	Active
Legal	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)
Adopted	August 26, 2013
Last Revised	May 11, 2015

The district recognizes that students desire to use their own computer or electronic storage device(s) in connection with classroom learning and school activities.

Allowing students to use their personal devices such as laptops, tablets, or smartphones will create efficiencies and enable students to employ additional computing resources beyond those available and provided by the district. Allowing students to use their personal devices for school purposes is a value and privilege provided to students at the district's discretion.

The benefits of personal device use must be weighed against the risks associated with such use. Limitations and controls on student use of personal devices for school purposes must be employed to address potential risks and strike an appropriate balance. This student personal device use policy sets the district's requirements and policies for student use of personal devices.

This policy applies to students who use their personal devices for connecting to, or accessing or interacting with, the district network or any district computer device.

GENERAL REQUIREMENTS

Personal Device Authorization

Only computer(s) or electronic storage device(s) that are authorized and registered may be used by students connecting to district resources. Students may not use prohibited personal devices to connect to Jeffco computing resources.

Authorization of a personal device for purposes of connecting to Jeffco computing resources is at the district's sole and absolute discretion. The district reserves the right to, and may deny or revoke (at any time, for any reason and without notice) authorization of a personal device and registration of a student as a registered user on the district's networks.

Personal Device Use Privilege

Student use of personal devices to connect to Jeffco computing resources is a privilege, not a right. Students who use their personal devices to connect to Jeffco computing resources are doing so voluntarily, and are not required to do so by the district. The student's use of personal devices to connect to Jeffco computing resources demands personal responsibility and an understanding of the appropriate handling of such devices, the data processed on them, and the acceptable and unacceptable uses of such devices. Failure to follow the use procedures contained in this policy and other relevant district policies may result in the loss of the privilege to use these devices to connect to Jeffco computing resources, as well as appropriate disciplinary action or legal action. The use of a personal device to connect to Jeffco computing resources is at the student's sole risk.

Prohibited Personal Devices and Uses

Personal devices that are prohibited from connecting to Jeffco computing resources include any computing device (including, but not limited to, any smartphone, laptop computer, netbook, desktop computer or tablet computer) that has been "jailbroken", tampered with, "modded" or modified in a manner prohibited or unintended by the manufacturer or seller of the device. The "unauthorized and unacceptable uses" section of the district's :student use of the internet and electronic communications: policy shall apply to Connected Personal Devices, and any reference in that section

to "district computers: or "district resources: shall be deemed to include Connected Personal Devices for purposes of this policy.

Responsibility for Personal Devices
The student who owns and is registered to use a Connected Personal Device is responsible for all activity related to, content stored, processed or transmitted on, the security of, and the use of, that personal device. If a student allows another to use a Connected Personal Device, the student is responsible for the use of that device when connected to Jeffco's computing resources.

Personal Device System Requirements, Configuration and Limitations
The district may set minimum system requirements such as approved operating systems, network protocols, and configurations for Connected Personal Devices. A personal device that does not meet such minimum system requirements may not access, interact with, or connect to the district network or any district computing resource.

Access to District Network
Connected Personal Devices must be registered and can only connect to the dictrict's computing resources via, approved processes established by the district.

Additional Applicable Policies and Standards
All use of personal devices must comply with all requirements set forth in other relevant district standards, policies, and procedures.

MONITORING AND PRIVACY

No Expectation of Privacy
Students agree and understand that personal devices used by students may contain, create or generate sensitive, personal, private or confidential information related to the student's (or others') use of the personal device, including but not limited to, account numbers, identification numbers, photos, videos, web-surfing history, chat history, personal emails, personally identifiable information, usernames, passwords and financial information. Students and other users of personal devices shall have no expectation of privacy when using or related to their use of personal devices when connected to Jeffco computing resources (such as devices being :Connected Personal Devices").

The district may at any time monitor, track, block, remove access to, any Connected Personal Device when connected to the district's computing resources, including without limitation the district's network; provided, however, that the district will only search the content stored on a Connected Personal Device in a manner consistent with applicable law and district policy JIH.

SECURITY OF PERSONAL DEVICES

No Shared Access to Personal Devices
Except for immediate family members, no person other than the registered user may be granted access rights, or access or use, a Connected Personal Device. Registered users must prohibit and prevent others from accessing a personal device.

Remote Access Software
Unless specifically authorized by the district in writing, software allowing for remote access to personal devices shall not be installed on and shall be removed from all Connected Personal Devices, including for example, and without limitation, Logmein, Webex and Gotomypc.

Operating System and Application Patching
Automatic operating system and application updating, and patching must be enabled for Connected Personal Devices when available, including without limitation for Windows operating systems, android, IOS, Adobe flash, Adobe Reader and Microsoft Office software. Students shall promptly install all relevant operating system and software security patches on Connected Personal Devices after they become available.

LAPTOPS, NETBOOKS and DESKTOPS

Antivirus Software
For all personal devices registered to connect to Jeffco computing resources that are laptops, netbooks or desktops (or similar devices), students shall install up-to-date anti-virus software designed to detect, prevent and remedy infection by malicious code, including without limitation, computer viruses, trojan horses, worms, and time or logic bombs. Such software will be configured to automatically: (i) update at least daily, including by obtaining and implementing the most current available virus signatures; and (ii) scan any file transferred into the district network for malicious code infection before transfer.

SECURITY INCIDENTS

Security Incident Reporting
Students must report any suspicious or abnormal behavior associated with their Connected Personal Device use to a staff member immediately who will then report to the District Information Security Department.

Investigation and Mitigation
When the district is informed of, detects or reasonably suspects a security incident related to a personal device registered to connect to Jeffco computing resources, including violations of district policy or laws, the district may require additional information from the student and/or further investigation. In addition, the district may undertake actions, or require the registered user to take actions, to contain, mitigate and remediate the security incident to protect both the interests of the student and the district. The district may disconnect a Connected Personal Device when it has a reasonable basis to believe that an incident involving a Connected Personal Device poses a threat to the security or integrity of the district network or any district computing resource, or any data stored, processed or transmitted thereon. The district may refuse to permit a personal device registered to connect to Jeffco computing resources from accessing, interacting with, or connecting to the district network or any district computing device until the registered user agreesto fully cooperate with the district's investigation and response to any security incident.

MISCELLANEOUS

Cooperation
Students shall cooperate, coordinate and assist the district with the actions it undertakes related to this policy and the district's implementation, maintenance and enforcement of this policy.

Support
Students are solely responsible for supporting their own Connected Personal Device, and software and data on such devices, and the district shall not, and has no responsibility to support any personal device, or software and data thereon. Students may not contact the district's support resources for district computer devices or the district network for purposes of receiving support or assistance with Connected Personal Devices or software or data thereon.

CROSS REFERENCES:

JIH, STUDENT INTERVIEWS, INTERROGATIONS, SEARCHES AND ARRESTS
JS, STUDENT USE OF THE INTERNET
JS-E1, ACCEPTABLE USE AGREEMENT, STUDENT USE OF THE INTERNET
JB, EQUAL EDUCATIONAL OPPORTUNITIES
EHAA, COMPUTER SECURITY