AR237.1 Attachment C - Best Practice Guidelines for Student Use of Chromebooks

BEST PRACTICES FOR CHROMEBOOK USE

Chromebook – refers to a Chromebook computer issued by the District to a District student for use in connection with the District academic program.

You are responsible for the appropriate use of your Chromebook both at school and at home. Chromebooks are issued to students for use for educational purposes. All commercial, illegal, unethical and inappropriate use of these Chromebooks is expressly prohibited.

1. You may not copy or duplicate copyrighted material. Copyright is the set of exclusive rights granted to the author or creator of an original work, including the right to copy, distribute and adapt the work. Copyrighted materials include books, maps, prints, musical compositions, dramatic works, photographs, paintings, drawings, motion pictures, computer programs, sound recordings, choreography and architectural works.
2. Downloading games, applications or software is expressly prohibited.
3. Data should not be stored on the Chromebook, but should be stored either in the District-provisioned cloud-based storage or on a removable storage device.
4. Do not loan your Chromebook to anyone, and do not share your "user name" or "password".
5. Always keep track of your Chromebook and take reasonable precautions to keep it safe.
    a. If you place your Chromebook in your locker make sure it is completely closed and locked.
    b. Since your backpack will be the primary storage for your Chromebook make sure that you never leave your backpack unattended.
6. When carrying your Chromebook always place it in the sleeve provided.
7. Do not place the power cord or adapter against the Chromebook screen in your backpack (the screen will break)
8. Be careful not to drop or fling your backpack (remember if it breaks, you may be held financially responsible)
9. If you notice that your Chromebook is working slowly or functioning in a strange or abnormal way, report it to the Technology Office.
10. Safe e-mailing:
    a. Don't open, forward or reply to suspicious e-mails. If you have a question about whether or not to open an e-mail, check with the Technology Department.
    b. Be wary of email attachments from people you don't know... it may be a virus or a malicious program.
    c. Never respond to e-mails that ask for personal information, such as your user name or your password.
    d. Think before you write and send an e-mail, be polite and courteous at all times.
    e. Almost all chain letters contain no useful information. This includes chain letters warning about viruses or Internet scams. Often the chain letters link you to viruses or are scams themselves. Don't pass them on.

f. Do not go to inappropriate / questionable web sites or click on questionable links as this may trigger a spam or computer virus attack.
g. The use of anonymous proxies or other technologies to bypass the JSD network filtering programs is prohibited.
h. When on school property, do not connect the Chromebook to the internet through any means other than the WIFI provided by the District through the JSD network.
i. When social networking, developing your personal web pages, or otherwise communicating with others consider the following:

    i. Be polite and courteous. Leave offensive text (i.e. curse words, insults, etc.) out of blog entries and comment postings to friends.
    ii. Once any text or photo is placed online it is completely out of your control, regardless of whether you limit access to your page. Anything posted online is available to anyone in the world.
    iii. You should not post or disclose information, photos, or other items online that could embarrass you, your family, or friends. This includes information, photos and items that may be posted by others on their page or on your webpage.
    iv. Do not post or disclose your personal information: addresses, phone number(s), date of birth, class schedules, your whereabouts or daily activities. You could be opening yourself up to online predators.
    v. Many potential employers, colleges and universities, graduate programs and scholarship committees now search these sites to screen applicants.

11. Saving Information:

a. Save your files in the cloud-based storage provisioned to you by the District. Additionally, you must ensure that important school information is separately backed up, either on a removable storage device or some other medium. The District is not responsible for loss of any data stored in District-provisioned cloud-based storage or on the Chromebook.
b. The JSD network administrator may review files and communications to maintain system integrity and ensure that students are using the system responsibly. Students and other JSD network users should not expect that email, information stored on Chromebooks, or other information stored in, transmitted through, or accessed through the JSD network, including, but not limited to cloud-based storage provisioned through the District, will be private.
c. Do not store any information on your Chromebook.
d. Any information on your Chromebook will be erased during the summer.

12. Other:

The District does not recommend plugging any additional personal devices into the Chromebook as this may cause problems with the Chromebook's operation. You are responsible for any damage to the Chromebook caused by any personal device you connect to the Chromebook.

AR237.1 Attachment C - Best Practice Guidelines for Student Use of Chromebooks

13. Remember, your Chromebook is your responsibility.

    Please be careful when using social networking sites and sharing personal information as this information may remain on the internet for years. Think before you act - after graduation would you want a prospective employer to view what you post?

The Superintendent or designee has issued administrative regulations containing guidelines to students for use of Chromebooks. Students should also refer to policies 815 *Acceptable Use of Internet, Computers, and Network Resources* and 237.1 *District-Issued Chromebooks.* Any violation will be subject to discipline as outlined in the applicable Student Handbook or Board Policy.

The District does not routinely monitor the JSD network for violations of school rules or District policies and is limited in its ability to monitor Chromebooks for cyber bullying and other violations. Therefore, if you have reason to believe that another student is using either the JSD network or their District-issued Chromebook in a manner that violates school rules or District policies, you are encouraged to report this to your Principal.