Kelso Student AUP: “Talking Points”

All Kelso students must have a signed AUP on record at their school in order to have computer and network access. Here are the major points to remember when signing the AUP. This document is for teachers to use in discussions with students. It is not intended to take the place of the AUP, and students should still review the entire document before signing. Please be aware that violation of these expectations may result in student loss of network use privileges, disciplinary actions up to and including suspension.

1. **Keep it School Related and Appropriate:** When using district technology resources (hardware, Internet, cameras, scanners, printers, etc.) the majority of the activities should be school-related and be conducted in an appropriate and ethical manner. For this reason personal e-mail, chat rooms, and social networking sites have been blocked by the district’s filtering software. *Attempts to bypass the district filter will result in disciplinary action*. Only district provided e-mail accounts are allowed at school. Illegal, inappropriate, bootleg, or copyrighted materials should not be downloaded onto school computers, shared with others, or stored in your folder on the server or in your Google Drive. School computers and network access cannot be used for commercial purposes, financial gain, or political lobbying.
2. **It’s not Private:** Be aware that all computer and network activity can be subject to monitoring and review. That includes Internet usage and any files that exist in your Google Drive account, on your folder on a school computer, or the server. The network administrator has the ability to monitor Internet usage on all district computers. Server folders or Google Drive accounts are subject to review if there is a suspicion of inappropriate material being stored there. If you accidentally access inappropriate material, turn off the computer monitor or close the laptop, and immediately notify your teacher.
3. **Be Careful What You Publish:** All web pages, blogs, wikis, or other online publishing that is being created as part of a school project needs to be done so under the supervision of a classroom teacher or advisor. Precautions should be taken to make sure student information is protected and students or the public are not allowed to publish anonymous, un-moderated content to WebPages that are used for school purposes. Do not plagiarize works found on the Internet.
4. **Keep it secure/respect privacy:** Do not share logon information with other students for any of your district or cloud based accounts. If you do so, you run the risk of having your files vandalized or deleted. You should not attempt to access files or data that do not belong to you by logging in as someone else, including staff members.
5. **Respect the Limits:** Delete unwanted files stored on district servers. Limit web streaming activities and downloads during times of heavy network use. Do not store large files (music, video, or exe files) unless they are part of a school project. Folders that exceed the file limit may have these types of files deleted from them by the building computer technician. Do not install unapproved or unlicensed hardware/software onto the network computers (wireless links, webcams, Skype, etc.). There should not be an expectation that files stored on servers or in district Google Drive accounts will remain accessible after students leave the district. It is your responsibility to transfer files to non-district account when you leave the district.
6. **Treat equipment with respect**: Do not damage or vandalize the hardware or Network by any means , or attempt to access computer files or settings that you are not authorized to access.
7. **Don’t Bully**: District computer resources should not be used to harass, intimidate, or bully others. This includes posting messages, making threats, or publishing text or images meant to harm others.