

## Administrative Procedure 140 – Appendix

---

### INTERNET ACCEPTABLE USE GUIDELINES

Students shall not:

- View, send or access abusive, obscene or harassing materials. A good rule to follow is never view, send or access materials which you would not want your teachers and parents to see. Should students encounter such material by accident, they are to report it to their teacher immediately.
- Access or participate in chat rooms or multi-user environments.
- Download or play games, participate in dating sites, subscribe to or access list servers, download music files or check send or receive email unless prior permission is granted by a teacher.
- Access, download or print game cheat codes.
- Share Internet passwords. If you are assigned a password, it is to be used by you only.
- Post messages to bulletin boards or other sites unless prior permission is granted by a teacher.
- Give out any personal information including names, addresses, phone numbers, email addresses or credit card information pertaining to themselves or any other person without appropriate staff approval.
- Engage in any commercial, for-profit activities.
- Violate copyright laws. Materials accessed through the Internet must be properly cited when referenced in a student research assignment.
- Download or install any commercial software, shareware or freeware onto network drives or disks. Do not copy other people's work or intrude into other people's files.
- Waste school resources by printing excessively or consuming limited hard drive space or network space.
- Use the Internet in any way which disrupts the service or its operation for others.
- Intentionally damage computers, computer systems or computer networks. Students should take special care with the physical facilities, hardware, software and furnishing. Students and staff may not remove/move, unplug, alter or add network related equipment or software to the network without the approval of the network administrator.
- Create or willfully disseminate computer viruses. Students are to be sensitive to the ease of spreading viruses and are to take steps to ensure that disks and files are virus free.

- Attempt to gain unauthorized or illegal access to Division technology resources or any other technology resources.
- Attempt to gain access to the Division or any other computer system or go beyond your authorized access by entering another person's password or accessing another person's file.
- Download, install or run any software without the express permission of your teacher or the network administrator.
- Alter the computers or change the settings or system configurations in any way.
- Alter, damage or vandalize District technology equipment or software in any way.
- Use Division resources to create, manage or access personal web pages which are not related to the educational goals of the Division.

Personal technology equipment brought to school is subject to the procedures outlined in the Student Technology Use Agreement.

Users have the responsibility to use technology resources in an appropriate manner. Consequences of misuse or abuse of these resources, depending upon the severity of the situation may include one (1) or more of the following:

- A warning, followed by re-clarification of the appropriate use guidelines.
- Loss of access to Division technology resources for thirty (30) days.
- Notification of parents and administrators by phone or personal conference.
- Referral to proper authorities for disciplinary and/or legal action.
- Students who have lost Internet or network privileges may not use personal equipment in lieu of Division or school equipment.

Reference: Sections 85, 87, 108, 109 Education Act