Bloomfield Public Schools
Student Technology Acceptable Use Guidelines

Purpose

The District's Student Technology Acceptable Use Guidelines are designed to inform students and parents of the school's requirements, expectations, and student's obligations when using district computers. These guidelines cover all technology including computers, interactive white boards, scanners, cameras and the district wired and wireless network, as well as computer accessories and software. We expect our students to use the computers responsibly by following these guidelines:

Personal Safety

- The district employs Internet content filtering and monitoring that is compliant with the Children's Internet Protection Act.
- All student computer use must be supervised.
- Pictures of students used in district communications will not provide information identifying any student without prior permission.
- Although students have cellular telephones in school, they may not be used in the buildings to place or receive telephone calls and text messages, access the district network, take pictures, or record audio or video.

Ethical Computing

Use of technology is ingrained in our daily activities and our goal is to provide students with access to 21st century knowledge that facilitates the pursuit of academic excellence and provides the skills necessary for lifelong learning. The district provides equipment and services strictly for educational pursuits; students are expected to follow generally accepted rules of network etiquette. These include, but are not limited to, the following:

- Be polite. Do not become abusive in your communication with others.
- Use appropriate language. Do not swear or use vulgarities or any other inappropriate language
- Keep personal information, including the logins, passwords, addresses, and telephone numbers of students or staff confidential.
- Use technology resources so as not to disrupt service to other system users. Do not upload post, e-mail, transmit, or otherwise make available any content that is unlawful, dangerous or may cause a security risk.

System Security

The district reserves the right to monitor and review any material on any machine at any time to determine any inappropriate use of network services. Students are provided with network accounts to access their saved files and teacher-assigned network resources. Students are responsible for the security of their computer equipment, files, and passwords. Students will keep their passwords private and not go beyond their authorized access to gain further access to the district network, other computer equipment or software including the files or accounts of others.

- Students will not disrupt or attempt to damage or disrupt any computer, system, system performance, or data.

- Students will not create, access or disseminate proxy sites for the purpose of bypassing content filtering.
- Students will promptly notify a teacher of security problems.
- Students will not use personal electronic devices in the schools without permission from a building administrator or his/her designee.
- Students have no expectation of privacy in files, disks, or documents that have been created in, entered in, stored in, downloaded from, or used on district equipment or resources.

<u>Inappropriate Conduct</u>

Network services are designed to support school operations. Disrupting these services either intentionally or through negligence is not acceptable. Examples of inappropriate use include:

- Illegal or malicious use, including downloading or transmitting of copyright material.
- Use of racial, sexual, or other harassment in violation of district policy.
- Accessing, viewing, or transmitting pornographic or obscene material.
- Disrupting the work of other users. This includes the propagation of computer viruses and use of the Internet to make unauthorized entry to any otherwise unapproved resource. (hacking)
- Intentionally spreading computer viruses or programs that loop repeatedly, or for the purpose of infiltrating a computer without authorization or damaging or altering without authorization the software components of a computer or computer system.
- Downloading unauthorized games, programs, files, electronic media, and/or stand-alone applications from the Internet that may cause a threat to the network.
- Disconnecting or rerouting network cabling or equipment.

<u>Appropriate use of materials</u>

We respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by copyright. Contact your teacher if you are unsure whether material is copyrighted.

The district has taken precautions to restrict access to inappropriate materials through a filtering and monitoring system. However, it is impossible to control access to all data which a user may discover. It is the user's responsibility not to initiate access to inappropriate material. Any site or material that is deemed inappropriate should be reported immediately to the teacher.

<u>District Hardware and Software</u>

Students assigned district hardware must take care of the equipment, ensuring its security when not in use. Students will be charged for damage to District hardware if it is determined care was not exercised. This includes laptops, printers, PDAs, iPods or any other electronic hardware issued to the student.

Only district-approved district software may be loaded on the equipment.

Only district owned or leased equipment will be permitted to run on the network; all unauthorized equipment will be confiscated.

<u>Discipline</u>

Students who engage in unacceptable use may lose access to the district computers and may be subject to further discipline in accordance with the student code of conduct.