FILE: GBCAB

MEDFORD AREA PUBLIC SCHOOL DISTRICT

DATE ADOPTED: July 19, 2001 **FILE SECTOR: PERSONNEL**
DATE REVISED: October 20, 2005 **POLICY TITLE: NETWORK USE – STAFF**
DATE REVISED: October 29, 2012
DATE REVISED: October 29, 2018

Medford Area Public School District (MAPSD) provides network access. These resources will be integrated where appropriate in the PreK-12 curriculum. As users of MAPSD network resources, it is essential that each user recognize their responsibility in having access to vast services, sites and people. The user is ultimately responsible for their actions in accessing network services and for adhering to district use policies, procedures and guidelines.

For this policy, network is defined as the district's servers and internet.

In the environment of a network, it is impossible to control all material. MAPSD believes that the valuable information and interaction available on this network far outweigh the possibility that staff may procure material that is not consistent with the educational goals of the district. Focus is in providing individual students with the understanding and skills needed to use the network in ways appropriate to their educational needs.

Through network access, staff may:

- Access resources.
- Enter into partnerships to enhance their learning options.
- Broaden their problem-solving and decision-making abilities.
- Broaden their research capabilities by using primary materials.
- Develop their higher-level thinking skills.
- Gain an employability skill needed for the 21st century.
- Utilize a personalized, motivational learning opportunity.
- Differentiate and assess available resources.

Policy Statements

Access to the network and resources within MAPSD is a privilege, not a right. This privilege will be revoked at any time. Furthermore, unacceptable use may result in suspension or revocation of network privileges and possibly other disciplinary action up to and including discharge from employment.

Users shall not access or use email or other computerized communication systems to relay threatening, intimidating, abusive or harassing messages. Such use may result in criminal sanctions consistent with state law.

Users shall not impose their choices on others, access private files, attempt to break security systems, copy software illegally, or use computer supplies that are not for school-related activities.

Users accessing district network systems may not corrupt network integrity by deliberately allowing inappropriate and/or dangerous files (i.e. viruses) to enter the system.

Any use of the network to facilitate illegal activity is prohibited and will be reported to the appropriate authorities.

Copyrighted material may not be placed on the network without the copyright owner's permission.

Users are responsible for the ethical and educational use of their own accounts. These accounts are to be used only by the authorized owner of the account for the authorized purposes. Users shall not intentionally obtain copies of and/or modify files or passwords belonging to other users.

The district is not responsible for the accuracy or quality of information obtained through its network service. The district is also not responsible for any damages the user suffers, including loss of data resulting from delays, non-deliveries, mis-deliveries, hardware system problems or service interruptions. Use of any information obtained via district technology is at the user's risk.

Principals may establish additional rules and procedures that they deem necessary to insure proper use of the network in their buildings.

Staff has the responsibility of making the educational goal clearly understood to the student. In addition, it is the responsibility of staff to inform students of their responsibilities when accessing the networks and the proper etiquette for their use.

Responsibility and Consent

Though the district does employ some types of filtering software it does not have complete control of information on the network. Therefore, information which users have access to may include material that is illegal, defamatory, inaccurate or potentially objectionable to some people.

The user is responsible for their actions using the network. Unacceptable uses may result in disciplinary action. Typical types of unacceptable use may be, but are not limited to, accessing for personal monetary gain, pornography, endangering the health/safety of others, gambling, union activity and/or use in any manner so as to cause damage or disruption to the system (but shall not pre-empt non-profit personal use such as accessing personal email.) MAPSD administration will determine what is "unacceptable use" and such decisions are final.

CROSS REFERENCE: **IIBGA~~A~~, IIBGB, IIBGC, KGA, & Employee Handbooks**
LEGAL REFERENCE: **§118.13, §120.18, §121.02(1)(H), §947.0125, §948.12 Wis. Stats., PI 8.01(2)(h), PI 9.03 of the Wisconsin Administrative Code, COPPA 16 CFR §312.6, 312.7, ACT 7 (18 U.S.C. §2252), 17 U.S.C. §512, CIPPA (47 U.S.C. §254 (h), (l)).**