Administrative Regulation

4612.00-R(2)
Page 1 of 4

TECHNOLOGY AND THE DISTRICT NETWORK AND INTERNET

A. All account holders on the Ingham Intermediate School District Network will be
    granted appropriate access to services the network offers. The following people may
    hold accounts and are considered account holders on the IISD Network:

    1. Students. Students who are currently enrolled in the district’s programs may
       be granted a network account upon agreement to the terms stated in this
       administrative regulation and supporting building level policies.

    2. Faculty, Staff and Board Members. Staff members currently employed by the
       district may be granted a network account upon agreement to the terms stated
       in this policy.

    3. Partners. Upon approval of the Information Technology Services department
       and Human Resources, staff members from constituent districts, contractors
       or contract employees, temporary staff, vendors, or others may be given a
       network account in order to complete tasks on behalf of and/or collaborate
       with Ingham ISD staff for the purpose of completing Ingham ISD work.

B. RIGHTS. In order to facilitate teaching and learning, enhance educational information
    exchange, and/or complete school district business, account holders have the right:

    1. To use all authorized technology (hardware, software, etc.) for which they
       have a need to perform their district responsibilities.

    2. To access information from outside resources.

    3. To access district networks and the Internet.

    4. To sign up for listservs and request newsgroups.

C. RESPONSIBILITIES. Account holders are responsible for:

    1. Using district technology only for facilitating teaching, learning, and enhancing
       educational information exchange consistent with the purposes of the district.

    2. Using the district telephones, mobile communication devices, and e-mail
       system for business use.
3. Working with the Information Technology Services or other departments to receive appropriate trainings as needed.

4. Adhering to the rules established for the use of technology in the district or through remote access outside of the district.

5. Maintaining the privacy of passwords (account holders are strictly prohibited from publishing or discussing passwords).

6. Having all storage devices scanned for virus, or other contamination which might endanger the integrity of district technology before they are used in district systems.

7. All material received via the district network under their account. They accept responsibility for keeping all inappropriate files and material, or files dangerous to the integrity of the district's networks, equipment, or software from entering the school via the district network or from being reproduced in visual, digital, or written format.

8. Maintaining the integrity of the network and e-mail system, reporting any violations of privacy and making only those e-mail contacts, which facilitate learning and enhance educational information exchange. Account holders are expected to abide by the district’s records management guidelines as it pertains to electronic records retention. Account holders do not have an expectation of privacy in their use of district technology. The district reserves the right to monitor, examine, and evaluate any and all use of district technology including but not limited to files, data, and electronic messages of any kind.

9. Adhering to all applicable copyright laws and guidelines in the use of technology and resources and in the transmission or copying of text or files on the Internet or from other resources. Copyrighted material must not be placed on any system connected to the district network without the author’s permission. Only the owner(s) or persons they specifically authorize may upload copyrighted material to the network. Account holders may download copyrighted material for their own use with the expressed permission of the owner or authorized person.

D. ACCOUNT HOLDERS ARE PROHIBITED FROM:

1. Using district technology for personal gain, for product advertisement or political lobbying, or for making any unauthorized financial commitments via the district network. Commercial use of district technology is strictly prohibited unless prior written consent from the system administrator has been granted.
2. Using the e-mail groups such as District All, TEC All, CACC All, MWS All, St. Vincent All, or HWS All to send e-mails containing chain letters, jokes, items for sale such as tickets, cars or for other personal purposes. Discretion is advised when using e-mail groups to inform staff about illness or death. Sometimes individuals prefer not to be acknowledged in this manner.

E-mails regarding news, events, fundraisers that benefit the community rather than the individual and are acceptable in a business setting are permitted.

3. The malicious use of district technology to disrupt the activity of others, to harass or discriminate against others, and to infiltrate unauthorized computer systems.

4. Accessing or accepting material or files inappropriate or dangerous to the integrity of the district's networks and equipment or software.

5. Any action that is determined by their supervisor, Information Technology Services, or Human Resources, constitute an inappropriate use of district technologies or improperly restricting or inhibiting other account holders from using district resources. Account holders specifically agree not to submit, publish, or display on district technology any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, or illegal material; nor shall they encourage the use of controlled substances. Transmission of material, information or software in violation of any local, state or federal law is prohibited.

6. Connecting non-district computing devices to the district network. Non-district computing devices are permitted to connect to the district wireless public network. Use of non-district computing devices on the public network must abide by all district policies and procedures.

7. Using district technology, including mobile communication devices for personal use.

E. CONSEQUENCES OF INAPPROPRIATE NETWORK BEHAVIOR:

1. Any account holder who does not comply with the technology and information access and use policy 4612.00 will lose technology privileges. Repeated or severe infractions of the policy may result in permanent termination of privileges. Note – it will still be the staff members responsibility to complete all aspects of their work regardless of suspension of privileges.
2. The Information Technology Services department may close an account at any
time for infractions of the policy and/or supporting building level access/use
policies and their decision is final. Only the superintendent may set aside the
decision if good cause is shown.

3. Account holders violating any of these rights and responsibilities may face
additional disciplinary action deemed appropriate in keeping with the
disciplinary policies and guidelines of the district, up to and including
discharge.

4. Student account holders violating any of these rights and responsibilities will
be dealt with according to the discipline policies of the individual school
buildings, local district and Ingham Intermediate School District.

5. The Information Technology Department may monitor any and all activity on
the district network and inspect any files, including e-mail, when required to do
so by law or deemed necessary by district administrators.

F. MISCELLANEOUS:

1. Non-district computing devices are permitted to connect the district wireless
public network. Use of non-district computing devices on the public network
must abide by all district policies and procedures.

G. ACCOUNT HOLDER RESPONSIBILITY DECLARATION:

1. Access and use of district technology is a privilege for the account holders.
The IISD has developed policy 4612.00 for local and wide area networks,
computer, and related equipment.

H. 1. Pursuant to Federal law, staff and students shall receive education about the
following:

a. Safety and security while using e-mail, chat rooms, social media, and other
forms of direct electronic communications
b. The dangers inherent with the online disclosure of personally identifiable
information
c. The consequences of unauthorized access (e.g. “hacking”, “harvesting”,
“digital piracy”, “data mining”, etc.), cyberbullying and other unlawful or
inappropriate activities by students online, and
d. Unauthorized disclosure, use, and dissemination of personally-identifiable
information regarding minors.
ADMINISTRATIVE REGULATION

Approved: July 28, 1997
Amended: October 21, 2002
          December 1, 2004
          March 25, 2005
          January 20, 2009
          August 19, 2010
          April 2, 2013
          June 18, 2013
          February 20, 2018