



Received: December 16, 2015

EMID 6067 Procedure 524A

## **524A COMPUTER ACCESS AND INTERNET USE AND SAFETY PROCEDURE**

### **I. UNACCEPTABLE USES**

- A. The following uses of the EMID system and Internet resources or accounts are considered unacceptable:
1. Users will not use the EMID system to access, review, upload, download, store, print, post, receive, transmit or distribute:
    - a. pornographic, obscene or sexually explicit material or other visual depictions that are harmful to minors;
    - b. obscene, abusive, profane, lewd, vulgar, rude, inflammatory, threatening, disrespectful, or sexually explicit language;
    - c. materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination (except when used for research and academic lessons);
    - d. materials that use language or images that are inappropriate in the education setting or disruptive to the educational process (except when used for research and academic lessons).
  2. Users will not use the EMID system to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks. Users shall not use district e-mail as part of a political campaign to support or oppose a political issue or the nomination or election of a candidate for public office except as otherwise agreed upon in school district employment agreements.
  3. Users will not use the EMID system to engage in any illegal act or violate any local, state or federal statute or law.
  4. Users will not use the EMID system to vandalize, damage or disable the property of another person or organization, will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means, will not tamper with, modify or change the EMID system software, hardware or wiring or



take any action to violate EMID's security system, and will not use the system in such a way as to disrupt the use of the system by other users.

5. Users will not use the EMID system to gain unauthorized access to information resources or to access another person's materials, information or files without the implied or direct permission of that person.
6. Users will not use the EMID system to post private information about another person, personal contact information about themselves or other persons, or other personally identifiable information, including, but not limited to, addresses, telephone numbers, school addresses, work addresses, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.
  - a. This paragraph does not prohibit the posting of employee contact information on EMID webpages or communications between employees and other individuals when such communications are made for education related purposes (i.e. communications with parents or other staff members).
  - b. A user is specifically prohibited from utilizing the EMID system to post personal information about a user or another individual on social networks including, but not limited to, social networks such as "Twitter" and "Facebook."
7. Users must keep all account information and passwords on file with the Office Manager. Users will not attempt to gain unauthorized access to the EMID system or any other system through the EMID system, attempt to log in through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user. Messages and records on the EMID system may not be encrypted without the permission of the Executive Director.
8. Users will not use the EMID system to violate copyright laws or usage licensing agreements, or otherwise to use another person's property without the person's prior approval or proper citation, including the downloading or exchanging of pirated software or copying software to or from any school computer, and will not plagiarize works they find on the Internet.
9. Users will not use the EMID system for conducting business, for unauthorized commercial purposes or for financial gain unrelated to



EMID mission. Users will not use the EMID system to offer or provide goods or services or for product advertisement. Users will not use the school district system to purchase goods or services for personal use without authorization from the Executive Director.

10. Student use of the Internet without direct staff supervision is not allowed.
  11. Users will not connect equipment that is not owned, maintained, and secured by EMID to district technology and/or networks including but not limited to personal laptops. Personal peripherals (i.e. computers, external hard drives, etc.) shall not be attached to district workstations without prior authorization from the Executive Director
- B. A student or employee engaging in the foregoing unacceptable uses of the Internet when off EMID premises may also be in violation of this policy as well as other EMID policies. Examples of such violations are, but are not limited to, situations where the EMID system is compromised or if an EMID employee or student is negatively impacted. If EMID receives a report of an unacceptable use originating from a non-school computer or resource, EMID may investigate such report. Students or employees may be subject to disciplinary action for such conduct including, but not limited to suspension or cancellation of the use or access to EMID's computer system and the Internet and discipline under other appropriate EMID policies, including suspension or exclusion from programs, or termination of employment. If appropriate, such use of the Internet may be reported to law enforcement for investigation.
- C. If a user inadvertently accesses unacceptable materials or an unacceptable Internet site, the user shall immediately disclose the inadvertent access to the Executive Director or program advisor. In the case of an EMID employee, the immediate disclosure shall be to the Executive Director. This disclosure may serve as a defense against an allegation that the user has intentionally violated this policy. In certain rare instances, a user also may access otherwise unacceptable materials if necessary to complete a project and if done with the prior approval of and with appropriate guidance from the Executive Director or program supervisor.

## **II. FILTER**

- A. With respect to any of its computers with Internet access, EMID will monitor the online activities of minors and employ technology protection measures during any use of such computers by minors and adults. The technology protection measures utilized will block or filter Internet access to any visual depictions that are:
1. Obscene;
  2. Child pornography; or



3. Harmful to minors.
- B. The term “harmful to minors” means any picture, image, graphic image file, or other visual depiction that:
1. Taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; or
  2. Depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and
  3. Taken as a whole, lacks serious literary, artistic, political, or scientific value to minors.
- C. Software filtering technology shall be narrowly tailored and shall not discriminate based on viewpoint.
- D. An administrator, supervisor or other person authorized by the Executive Director may disable the technology protection measure, during use by an adult, to enable access for bona fide research or other lawful purposes.
- E. EMID will educate students about appropriate online behavior, including interacting with other individuals on social networking websites and in chatrooms and cyber bullying awareness and response..

### **III. NO EXPECTATION OF PRIVACY**

- A. By authorizing use of its system, EMID does not relinquish control over materials on its system or any files or datum on its system. Users do not have a reasonable expectation of privacy in the contents of any file or datum on the EMID system.
- B. Routine maintenance and monitoring of the EMID system may lead to a discovery that a user has violated this policy, another district policy, or the law.
- C. An individual investigation or search will be conducted if EMID authorities have a reasonable suspicion that the search will uncover a violation of law or district policy.
- D. Parents have the right *to* review the contents of their child’s files and e-mail files. Parents have the right to request the termination of their child’s individual account at any time.



- E. EMID employees should be aware that the district retains the right at any time to investigate or review the contents of their files and e-mail files. In addition, EMID employees should be aware that data and other materials in files maintained on the district system may be subject to review, disclosure or discovery under Minn. Stat. Ch. 13 (the Minnesota Government Data Practices Act).
- F. Software, hardware, or other peripherals connected to the EMID system may be confiscated by the district.
- G. EMID will cooperate with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with EMID policies conducted through the EMID system.

#### **IV. ELECTRONIC RECORD RETENTION – EMAIL MESSAGES**

Email messages are potentially official government records. All email messages that fall under the “correspondence” category will be archived according the School District General Records Retention Schedule of the State of Minnesota.

District emails is stored for a period of three years from date of receipt through a backup process. The archiving of messages deemed as official records beyond three years will be the responsibility of the individual users. Any message can be retrieved during that time period.

#### **V. SOCIAL MEDIA**

- A. EMID recognizes the importance of using social media as a communication and learning tool. Social media includes websites and applications where users share and create content and includes blogs, wikis, podcasts, virtual worlds, and social networks.
- B. All staff are expected to serve as positive ambassadors for EMID and appropriate role models for students. It is vital that staff maintain professionalism in their interactions with students and the community. Failure to do so could put the employee in violation of existing EMID policy and at risk of disciplinary action.
  - a. Always an EMID employee. The lines between public and private, personal and professional are sometimes blurred in the digital world. Whether is it clearly communicated or not, employees will be publicly identified as working for and sometimes representing EMID in what is done and said online. Staff must always write in the first person and make it clear they are speaking for themselves and not on behalf of the district. Staff must never share confidential information; posts can easily be shared by others.



- b. Professionalism. Ideas must be expressed in a respectful manner. Respect copyright and fair use guidelines. Do not use any EMID logo or image without permission from the Executive Director.
- c. Respect others. Staff may not post offensive comments about students, colleagues, or EMID in general. Negative comments about people may amount to cyber-bullying and could be deemed a disciplinary offense. Permission should be sought when posting photos or movies of staff or students (when personally identifiable) when possible.
- d. Staff student relationships. Staff are prohibited from establishing personal relationships with students that are unprofessional and thereby inappropriate. Unprofessional relationships include writing personal letters, email or text messages; calling students on cell phones or allowing students to make personal calls to you unrelated to EMID work; sending inappropriate pictures to students; discussing or revealing inappropriate personal matters about your private life or inviting students to do the same; engaging in sexualized dialogue in any form. Inappropriate or offensive content posted to social networks by staff and viewed by students, parents, or other staff may be investigated by the Executive Director and, if warranted, may result in disciplinary action. District email is not private. All communication by staff to students or parents at any time from any email system shall be expected to be professional. Email between staff and students and parents shall be done through the school provided email application and must conform to district email policies.
- e. Personal Use. Staff must not use EMID contact information (email, address, phone, etc.) when using social media for personal use. Staff must not connect with students via personal social media. Staff must not use EMID equipment or the district network as primary tools for maintaining personal accounts.

## **VI. INTERNET USE AGREEMENT**

- A. The proper use of the Internet, and the educational value to be gained from proper Internet use, is the joint responsibility of EMID students, parents, and employees.
- B. This policy requires the permission of and supervision by the program's designated EMID staff before a student may use a school account or resource to access the Internet.
- C. The Internet Use Agreement Form for students must be read and signed by the user, the parent or guardian, and the program supervisor. The Internet Use



Agreement Form for employees must be signed by the employee. The form must then be filed at the district office.

## **VII. LIMITATION ON SCHOOL DISTRICT LIABILITY**

Use of the EMID system is at the user's own risk. The system is provided on an "as is, as available" basis. EMID will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on any data storage device (i.e. compact disk, digital video disk, hard drives, servers, etc.) or for delays or changes in or interruptions of service or misdeliveries or nondeliveries of information or materials, regardless of the cause. EMID is not responsible for the accuracy or quality of any advice or information obtained through or stored on the district system. EMID will not be responsible for the loss or damage to district owned computer hardware, software, or related electronic equipment issued to an EMID employee when such loss or damage occurs in use outside of the employee's regular duties and work responsibilities. EMID will not be responsible for financial obligations arising through unauthorized use of the district system or the Internet.

## **VIII. USER NOTIFICATION**

- A. All users shall be notified of EMID policies relating to Internet use.
- B. This notification shall include the following:
  - 1. Notification that Internet use is subject to compliance with EMID policies.
  - 2. Disclaimers limiting the EMID's liability relative to:
    - a. Information stored on any data storage device.
    - b. Information retrieved through district computers, networks or online resources.
    - c. Personal property used to access district computers, networks or online resources.
    - d. Unauthorized financial obligations resulting from use of district resources/accounts to access the Internet.
  - 3. A description of the privacy rights and limitations of school sponsored/managed Internet accounts.
  - 4. Notification that, even though EMID may use technical means to limit student Internet access, these limits do not provide a foolproof means for enforcing the provisions of this acceptable use policy.



5. Notification that goods and services can be purchased over the Internet that could potentially result in unwanted financial obligations and that any financial obligation incurred by a student through the Internet is the sole responsibility of the student and/or the student's parents.
6. Notification that the collection, creation, reception, maintenance and dissemination of data via the Internet, including electronic communications, is governed by Policy 406, Public and Private Personnel Data, and Policy 515, Protection and Privacy of Pupil Records.
7. Notification that, should the user violate EMID's acceptable use policy, the user's access privileges may be revoked, a disciplinary action may be taken and/or appropriate legal action may be taken.
8. Notification that all provisions of the acceptable use policy are subordinate to local, state and federal laws.

#### **IX. PARENTS' OR GUARDIAN RESPONSIBILITY; NOTIFICATION OF STUDENT INTERNET USE**

- A. Parents and guardians bear responsibility for the same guidance of Internet use as they exercise with information sources such as television, telephones, radio, movies and other possibly offensive media. Parents and guardians are responsible for monitoring their student's use of the EMID system and of the Internet if the student is accessing the district system from home or a remote location.
- B. Parents or guardians will be notified that their students will be using EMID resources/accounts to access the Internet and that the district will provide parents or guardians the option to request alternative activities not requiring Internet access. This notification should include:
  1. A copy of the user notification form provided to the student user.
  2. A description of parent/guardian responsibilities.
  3. A notification that the parents / guardians have the option to request alternative educational activities not requiring Internet access and the material to exercise this option.
  4. A statement that the Internet Use Agreement must be signed by the user, the parent or guardian, and the program supervisor prior to use by the student.
  5. A statement that EMID's acceptable use policy is available for parental / guardian review.