Guidelines for Implementation of Acceptable Use Policy for Electronic Information, Communication, and Technology Resources

ACCEPTABLE USE POLICY AND GUIDELINES GENERAL INFORMATION

Enforcement of the policy

- The Employee Services Department is responsible for reviewing annually with Department Directors, Supervisors, and Principals the Acceptable Use Policy (AUP) and Acceptable Use Guidelines (AUG) documents.
- Employee Services presents the AUP/AUG to all new employees as part of the new employee orientation session.
- Employees are required to review and formally acknowledge, through a signed statement or web-based acceptance mechanism, the AUP/AUG documents annually.

Consequences of breach of policy

Use of Information, Communication, and Technology (ICT) resources is a privilege, not a right. The district recognizes that some personal use of district e-mail, voice mail, and computer systems - including use during non-work time is acceptable; however, excessive use or abuse of these privileges (as outlined in the AUP adopted by the school board) is unacceptable. Abuse of these privileges may result in one or more of the following consequences:

- Suspension or cancellation of use or access privileges
- Payments for damages or repairs
- Discipline under appropriate school district policies including suspension, expulsion, exclusion or termination of employment, or civil or criminal liability under applicable laws

Data Privacy

- By authorizing use of ICT resources, the District does not relinquish control over materials on the systems or contained in files on the systems. Files stored on school-based computers and communications via e-mail, Internet browsers, or voice mail are not private.
- Electronic messages and files stored on school-based computers may be treated like any other school property. Administrators, faculty, or network personnel may review files and messages to maintain system integrity and, if necessary, to ensure that users are acting responsibly.
- School district employees and students should also be aware that data and other material and files maintained on the school district system may be subject to review, disclosure, or discovery. The school district will cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with school district policies conducted through the school district system.
- All data on students maintained by the school, school district, or by persons acting for the school district are private and may be accessed or shared only with those having an educational need to know. The only exception is “directory information,” which has been designated by the district as public information unless specifically restricted by the individual. Directory information includes:
  - Name and photo
  - Name of school attended
  - Date of birth
  - Grade in school

- Participation in officially recognized activities and sports
- Awards and honors
- Weight and height of members of an athletic team
- Dates of attendance (enrollment dates)
- Last grade completed
- Date of graduation
- Immunization history

***Use of Copyrighted Material: ***printed with permission from the University of North Carolina at Chapel Hill
Compliance with federal copyright law is expected of all students, faculty, and staff at Anoka-Hennepin schools. “Copyright” is legal protection for creative intellectual works, which is broadly interpreted to cover just about any expression of an idea. Text (including e-mail and web information), graphics, art, photographs, music, and software are examples of types of works protected by copyright. The creator of the work, or sometimes the person who hired the creator, is the initial copyright owner.

All or part of a copyrighted work may be used only if (a) you have the copyright owner’s permission, or (b) you qualify for a legal exception (the most common exception is called “fair use”). “Use” of a work is defined for copyright purposes as copying, distributing, making derivative works, publicly displaying, or publicly performing the work.

Copying, distributing, downloading, and uploading information on the Internet may infringe the copyright for that information. Even an innocent, unintentional infringement violates the law. Violations of copyright law that occur on or using the District’s networks or other resources (copiers, computers, etc.) may create liability for the school district as well as the user. Accordingly, repeat infringers will have access privileges terminated.

DISTRICT NETWORK HARDWARE AND SOFTWARE GUIDELINES

Network Electronics

The district's Wide Area Network (WAN) infrastructure, as well as the building-based Local Area Networks (LANs) have been implemented with performance planning and appropriate security major parts of the process. Guarantees of an appropriate level of network efficiency, reliability, and manageability, along with acceptable use practices and most effective use of resources are foremost priorities of the Technology Steering Committee.

Modifications to an individual building network infrastructure and use will almost always affect LAN performance and quite often will have an impact on the efficiency of the WAN. For this reason, any additional network electronics including, but not limited to, switches, routers, and wireless access points are to be purchased, installed, and configured only by Network Services.

Network Devices

Before any network devices can be added to an individual building’s network, Network Services must grant permission. To gain this permission, a letter should be written to the supervisor of Network Services detailing the need and intended use.

In the case of servers, the letter must also include the information content of the server, along with the name and credentials of a staff member who ultimately will be responsible for the use, maintenance, and content of the server

Authorization of Building Remote Access

Staff wanting remote access to the district network must submit an application to the Network Services department. Upon approval of the application, Network Services will supply remote access to district computing resources. The remote access user must follow recommended security practices of the network, including the use of up-to-date antivirus software.

Basic Standards for Desktops and Laptop Computers

- Employing Active Directory when logging onto district computers and servers provides a high level of security when using district-defined password criteria (password requirements are addressed later in this document).
- Your computer should be secured whenever it is not in use by invoking the password on the computer and/or logging off the network. Leaving a computer open or logged in while you are away enables anyone to potentially access your grade book, e-mail, and other information-sensitive files.
- Desktop and laptop computers connected to the network must have an up-to-date version of antivirus software with current definition files.
- All district workstations should be completely powered off at the end of each workday.

Maintenance of Local Hard Drives

Situations do occur that require hard drives to be reformatted and erased.

- Only software considered part of the “district image,” which is consistent throughout the district, will be reinstalled.
- Approved software purchased by the building will need to be reinstalled by the building technology support staff. With this in mind, installation disks of specific school-purchased software should be kept in an identified location at your building.
- Unlicensed software will not be reinstalled, nor will we be able to retrieve personal data files from the local hard drive.
- Individuals are responsible for making backups of their data files.

Removable Media

All removable media (USB devices, external hard drives, CDs, flash drives, etc.) with sensitive data must be securely protected with a password or stored in a secure location.

Software and Hardware Purchases

Keep in mind that not all software available may work on our district computers or network. By the same token, not all hardware is compatible with our network. Therefore, it is essential that all curriculum areas, central departments, and site technology staff collaborate with Network Services, Desktop Services, and their Technology Facilitator before decisions involving purchases of hardware or software are made.

- Software should be ordered directly through the district Purchasing Department, using the TIES finance system. Information on standard district software can be found on the district website, Purchasing Department pages.
- No unlicensed software should be installed on district computers.
- For technology/hardware purchases, refer to the district website, Technology Purchasing pages. For items not listed on the website, contact your technology facilitator.

Passwords

All users that have access to the district WAN, either to access files on servers or to use the district e-mail system, must maintain a password for their account.

Users are not authorized to share their user name or password with other staff, except with authorized technology support staff. All users are required to change the default password assigned when their network account is created. In addition, all staff users must change their password every 120 days (this includes a 14-day reminder period) or on request from building technology support personnel.

Electronic Devices

The District defines electronic devices as, but not limited to, the following:

- Laptop and desktop computers
- Tablets
- Wireless e-mail and text-messaging devices, i.e., iPod
- Smart Phones

For purposes of this document, the term “Personal Electronic Device” refers to staff- or student-owned electronic devices.

District Electronic Device Standards and Support

District technology staff provides basic installation, synchronization, and specific software support for district electronic devices. District technology support staff includes the building’s technology teacher, technology para, and technology facilitator, as well as Network Services, Desktop Services, and Communications Technology Department staff. Buildings should purchase an extended protection plan (warranty) in situations where conditions promote breakage.

District electronic devices contain sensitive data, posing a security risk to both individuals and the school district. These devices also have the added risk of being stolen, misplaced, or left unattended. Therefore, password protection is required on all District electronic devices. In cases where the device is lost or stolen, the owner’s direct supervisor must be notified. If the user is using active sync with the device in order to check district email, the device owner and/or supervisor must inform the Communications Technology Department to ensure sensitive data can be removed from the device.

Staff-Owned Electronic Device Standards and Support

District technology staff are not responsible for supporting staff-owned electronic devices. Users can access their district e-mail using District-approved security protocols, which currently include https:// or SSL and are listed in the *Guidelines for Staff Access to District Resources from Outside District Facilities* which is maintained by the Technology and Information Services Department. Users requiring setup support on their device should contact their device provider. In all cases where staff are using personal electronic devices to access any District resources, including e-mail, staff are responsible for safeguarding the data by not sharing their user name and password with others and logging out of district resources when they are not specifically using them.

Student-Owned Electronic Device Use

The District is committed to providing students with a safe, secure, and positive learning and working environment. The use of portable electronic devices on school property can compromise or interfere with this goal; therefore, the use and possession of such devices must be regulated. Given the prevalence and exponential growth of the types of portable electronic devices available, the District, building administration, and teacher maintains the right to control the time, place, and manner in which electronic devices are used.

Parents/guardians are advised that the best way to contact their child during the school day is by calling the school office.

The possession, use, or sharing of electronic devices in locker rooms, rest rooms, or any other area that could constitute an invasion of any person's reasonable expectation of privacy is strictly prohibited. Any device used for such purposes shall be confiscated and searched by school personnel. Students are required to relinquish electronic devices to school personnel when directed. Refusal to comply with such directives will be considered insubordination and the student will be subject to disciplinary action.

Access Internet Resources on a personal electronic device

All buildings have a Guest wireless network. The "ISD11" wireless network is reserved for district electronic devices only, and should not be accessed by non-district electronic devices. Staff and students using their personal electronic devices may use the Guest wireless network for instructional and administrative purposes. Limited personal use of the District's Guest wireless network is permitted if the use:

- Poses no tangible cost to the District
- Does not unduly burden the District's computer or network resources
- Has no adverse effect on an employee's job performance or on a student's academic performance

Access to the District's electronic communications system is a privilege, not a right. Accepting the Terms of Service, the user shall abide by the regulations and guidelines.

Below are the guidelines for each of the grade levels and Special Education.

High School – Student Guidelines

Electronic devices may be used in the classroom with teacher or administrator approval. An electronic device may be used to make calls before or after school, during the individual student's assigned lunch, or during passing time. Taking pictures or video and audio recording other students or school staff is prohibited without the permission of a teacher or administrator per district guidelines. Electronic devices used without the appropriate approval may result in disciplinary action. Student removal of a memory chip or battery from a phone in the process of being confiscated is considered grounds for disciplinary action by school administration.

Middle School – Student Guidelines

Electronic devices may be used in the classroom with teacher or administrator approval. A portable electronic device may not be used to make phone calls or send text messages during the school day. Students wishing to use portable electronic devices for educational purposes outside the classroom must have teacher and/or administrator approval. Taking pictures or video and audio recording other students or school staff is prohibited without the permission of a teacher or administrator per district guidelines. Portable electronic devices used without the appropriate approval may result in disciplinary action. Student removal of a memory chip or battery from a phone in the process of being confiscated is considered grounds for disciplinary action by school administration.

Elementary School – Student Guidelines
At elementary school levels, electronic devices must be concealed and shall not be powered on or used in any way during regular operations of the school day, during other school-sponsored and supervised group activities during the school day (e.g., during student assemblies, field trips, events, or other ceremonies, etc.), or when their use is otherwise prohibited by school personnel.

Special Education
Access is based on individual student needs. If use of a portable electronic device is required in individual instances to assist a student with the student's education, as part of a student's Individual Education Plan (IEP), or as a part of a 504 plan, the use of such device must be documented within the student's IEP or 504 plan and communicated to building administration and staff.

Liability Statement
The district assumes no responsibility for loss or damage to personal electronic devices, whether in the possession of staff or students. Staff should make every attempt to store confiscated devices in a secure area. The Anoka-Hennepin School District bears no responsibility for, nor are its employees obligated to investigate, the theft of any personal electronic device.

INTERNET USE GUIDELINES

Use of Web tools:

- All Anoka-Hennepin teachers are encouraged to develop and maintain classroom Web sites as a way to communicate on an ongoing basis with students and parents/guardians. Teachers must use district-provided Web software for classroom Web sites to limit students' potential exposure to inappropriate material on the Internet and to ensure compliance with School Board policy regarding solicitation of students.
- All Anoka-Hennepin central departments are encouraged to develop and maintain a department Web site. Web sites must conform to district design standards and be up to date.
- Web announcements promoting a business are prohibited by district Solicitation Policy. The Superintendent/Associate Superintendents may make exceptions if benefits are judged sufficient to merit exception.

Student Internet Use:

Under the Children's Internet Protection Act (CIPA), districts are required to restrict minors' access to internet-based materials. The District has licensed a commercial internet filtering package that meets or exceeds the CIPA requirements for student protection.

Students using district-provided Internet access must first have the permission of and must be supervised by the district's professional staff. Students using district-provided Internet access are responsible for good behavior on line just as they are in a classroom or other area of the school. If students use their personal device using their own data plan (3G/4G), they will not be filtered by the district Internet filter. Inappropriate use of the Internet using a personal data plan will be subject to discipline. The same general rules for behavior and communications apply. Parents should be made aware of student Internet use by means of a written notice, perhaps in the student handbook or a student delivered handout.

COMMUNICATION TOOLS

Staff E-Mail

The district manages an e-mail system for staff business/communications purposes. All e-mail messages are retained on the system until deleted by the staff member. Staff are expected to remove old messages in a timely fashion; system administrators may remove such messages if not attended to regularly by the individual user.

Electronic messages stored on district servers are treated like any other school property. That said, system administrators will not intentionally inspect the contents of a user’s e-mail account or disclose such contents to other than the sender or intended recipient without the consent of the sender or intended recipient, unless required to do so by law or District policies, or to investigate complaints regarding e-mail which is alleged to contain material contrary to District policies.

Staff members are provided with district e-mail accounts to improve the efficiency and effectiveness of communication, both within the organization and with the broader community. Staff using e-mail to correspond with parents and students must adhere to the following:

- Staff must use a school-provided e-mail account for all parent and student communications. Use of a staff personal e-mail account for parent/student communication is not authorized.
- E-mail is not an effective medium for contentious, emotional, or highly confidential issues. These issues are more effectively dealt with through a phone call or personal meeting.
- E-mail messages to parents should be consistent with professional practices used for other correspondence. This includes grammar, format, and salutation.
- E-mail to students should be consistent with professional practices for other correspondence and may not include content of a personal nature.
- All e-mails that reside on the District servers are not confidential. E-mail messages may be requested by the public under the Right-to-Know Law and may, unless they are exempt under the law, be open to public inspection.
- E-mails should be short and directional in nature and include only the facts.
- Communicate only with parents at e-mail addresses listed in the Student Information System (SIS) unless steps have been taken to verify that the communication is occurring with a parent/guardian that has educational rights for the student.
- Communicate with students using only the e-mail address listed in the SIS. That e-mail address is the official, district-provided student e-mail account.
- Carbon copy parents on e-mails to students.
- Care should be given when using student names. Refer to students by first name, initials, or “your son/daughter,” depending on the content. Do not discuss nonrelated students.

Staff are required to:

- Check e-mail at least daily
- Respond to e-mail messages in a timely fashion, usually considered to be within 2 working days.

- Delete messages after reading them. If you need to keep messages for any reason, file them in personal folders rather than the Exchange server folders.
- Avoid sending enclosures larger than 1 MB. For large file transfers, used shared folders on building servers.
- Subscribe only to list services that are critical to your job responsibilities.
- Do not forward or otherwise respond to "chainmail" type communications.
- Do not respond to spam or phishing attempts by clicking on any links or providing any account information. Know that district network/communications staff will NEVER ask for account information via email.
- Do not send email messages to all staff. Messages you would like to send to all staff should be sent to the Communications and Public Relations Department for inclusion in staff e-newsletter if appropriate.

Student e-mail:

Secondary (grades 6 through 12) students will be provided district e-mail accounts through our Anoka-Hennepin Apps system to promote effective communication. District-provided student e-mail accounts are a privilege and district guidelines regarding the use of student e-mail must be strictly followed. Student e-mail accounts must be used for educational purposes only. If a student receives e-mail with libelous, defamatory, offensive, racist, or obscene remarks, they are required to retain the mail and report it to a teacher immediately.

Acceptable use of student e-mail includes:

- E-mail should be used to communicate with a teacher regarding assignments, class projects, and class activities.
- E-mail should be used to include links to share homework documents created in Google Docs with the teacher or fellow students. Enclosing documents in an e-mail is discouraged.
- E-mail communication between students should be used to facilitate collaboration, planning, and research for school-related projects and activities.
- E-mail is not confidential or private and can be ready by teachers or district personnel.

Unacceptable use of student communication includes:

- E-mail must not contain libelous, defamatory, threatening, offensive, racist, or obscene remarks.
- E-mail should not be forwarded without the senders' permission.
- Students cannot attempt to send e-mail from another person's account or attempt to impersonate another student's e-mail address.
- Students cannot forward spam, jokes, images, executable files, or viruses. Doing so will cause a loss of internet and e-mail privileges.
- Students cannot send inappropriate links, images, or executable files.

Student Google Web Sites:

Secondary (grades 6 through 12) students are provided access to Google Sites through the Anoka-Hennepin Apps system to promote effective communication and collaboration. District-provided student web sites are a privilege and district guidelines regarding the use of student created web sites must be followed. Student created web sites must be used for educational purposes only. Students can, upon graduation, transfer their Google Sites from their AHApps account to a personal account. Contact your technology teacher for instructions on how to transfer your digital portfolios.

Acceptable use of student created Google Sites includes:

- Google Sites used to communicate with a teacher regarding assignments, class projects, and class activities.
- Google Sites between students should be used to facilitate collaboration, planning, and research for school-related projects and activities.
- Google Sites are not confidential or private and can be read by teachers or district personnel.

Student created Google Sites should not include personal information including: addresses, birth dates, phone numbers, or personal identifiers.

Unacceptable use of student Google Sites includes:

- Google Sites that contain libelous, defamatory, threatening, offensive, racist, or obscene remarks.
- Google Sites with inappropriate links, images, or executable files.
- Google Sites for non-educational uses.

Electronic Transmission of Educational Data

When records containing educational records or private data are transmitted electronically, either by using e-mail or an FTP site, staff are expected to protect the privacy of the data by password-protecting the record or file. Staff are also expected to ensure records are sent only to individuals with a right to said records.

Telecommunications System

The district maintains a telecommunications system that has these features/capabilities:

- A phone in every classroom. To ensure our students are not interrupted during class time, this phone is accessed from within the district system only. Callers from outside the district cannot dial the classroom directly.
- Teachers/staff who do not have actual office space are assigned "phantom" phone numbers that can be programmed to ring any phone in the district. To ensure students are not interrupted during learning time, staff with phantom numbers should program their phone number to ring in the classroom only during non-student-contact times, such as a prep hour or before/after school is in session.
- Voice mail box for all staff members.

Staff are required to:

- Check voice mail daily.
- Return calls within 2 working days.
- Delete messages after listening to them.
- Record a greeting that includes, "If you need immediate assistance, please press zero." *This is mandatory because that "zero out" also directs 911 calls to the office in an emergency situation.*
- Record your name to ensure callers know that they have reached the correct voice mail box.

Use of Automated Calling System:

- Only the superintendent or a designee are authorized to make all-District calls.
- Only principals are authorized to make all-school calls except in emergency situations.
- Messages to specific groups within a school must be authorized by the principal.

- Overuse of the automated calling system (more than once a week) should be avoided except when needed for emergency messages.
- Messages related to district closure, including cancelation of after-school activities, or emergency situations must be authorized through the Communications and Public Relations Department to ensure a consistent message is being sent.

ENERGY MANAGEMENT

The District strives to reduce our environmental footprint by pursuing energy conservation efforts and practices. Staff and students attend instructional sessions regarding energy conservation best practices.

These guidelines are in place with regards to computers and monitors:

- All computers are to be powered off at the end of the day.
- Power management features are enabled on each computer.

POLICY/GUIDELINES LOGISTICS:

- Adoption: Committee, Superintendent, School Board
- Distribution: On paper and via the District website to staff; to students and parents/guardians in the Elementary Handbook and Secondary Handbook and on the district Web site; electronically on the district Internet Information Server.
- Revision: The Technology Steering Committee will periodically review and maintain these guidelines. Requests for guideline amendments should be forwarded to the Chief Technology and Information Officer for consideration by the committee.

Anoka-Hennepin ISD 11
Revised 6/25/2012