Technology

Rules and Regulations

Hillsboro R-3 School District

Technology Department

Adopted Summer 2009

Board Approved:

~~July 23, 2009~~

Modified by Board of Education
April 20, 2015

TECHNOLOGY RULES AND REGULATIONS

OVERVIEW

Technology Rules and Regulations include Cyberbullying, Automated Mass Communication, Email Archiving, Email Use, Email Retention, Internet Use (Employee & Student), Electronic devices, Password Usage, and Internet Safety.

Email Archiving

Hillsboro R-3 District email will be archived for the period of one (1) year. All archives will be maintained on an email or archive server. Once a month archive has been retained more than 12 months, it will be deleted at the end of the 13th month of retention.

All district email should be conducted on the district's approved email system. Personal email should not be used to conduct school business without prior approval by administrators in the Technology Department and Administration office.

Email Limitations

1. Email will expire and be deleted after it is 730 days old
2. Mailbox size is limited to 300 MB. You will be notified via email when your mailbox is 90% full. Once you receive this notification, it is important that you cleanup and delete email that is no longer needed. Groupwise displays the size of your mailbox.
3. Please limit use of district email for sending photos and images. Attachment size is limited to 16 MB per email.
4. Junk email is deleted after it is 7 days old.
5. Trash email is deleted after it is 14 days old.

Email Use

The Hillsboro R-3 School District email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.

District email system shall not be used for the purpose of personal financial gain (ex. Inviting individuals to a party for selling items, selling tickets to events, advertising a business, etc.).

Using a reasonable amount of Hillsboro R-3 School District resources for personal emails is acceptable, but it is encouraged to use a personal email account (examples include Yahoo, Google, Hotmail, etc.).

Sending chain letters or joke emails from a Hillsboro R-3 School District email account is prohibited.

Virus or other malware warnings and mass emailing about non-school business within our school district and emails from Hillsboro R-3 School District shall be approved by Hillsboro R-3 School District Director of Technology or Superintendent before sending.

Hillsboro R-3 School District employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Hillsboro R-3 School District may monitor messages without prior notice. Hillsboro R-3 School District is not obliged to monitor email messages.

Electronic Devices

STUDENTS: Electronic devices (i.e. Ipods, MP3 players, etc.) may not be used during the instructional day. Due to security issues, personal laptops & portable computer devices are not allowed at school. Only school owned computer devices are allowed for connectivity to the district's computer network. The electronic devices may be confiscated.

TEACHERS: Personal laptops and network devices (including wireless) may not be used during the instructional day and they are not allowed to be brought to school without prior approval by the building principal and the director of technology. Other personal devices (i.e. Ipods, MP3 players, personal organizers, etc.) are allowed to be used for personal use only, but these devices are not to be connected to any district technology including computers and network. If a device has wireless broadband access, CIPA guidelines are to be followed while the device is being used on campus. The use of electronic devices is subject to the school building policies.

Employee Internet Access Filtering

Filtering is determined by the Novell username login. All employees will receive less restrictive filtering if you log in as yourself. Please understand that any student login will receive the most restrictive filtering. If you use the "Workstation Only" login, you will be filtered like the students. Internet Access logs are retained for a period of one year and logs are organized by username, network IP address, and unique network MAC address.

(NOTE: Please understand that each building is responsible for defining when various Internet activity occurs, but it is recommended that the activities below and others should be done during planning periods, before/after school, and lunchtime.)

FAQ Acceptable uses include:

1. Personal financial banking and paying bills online
2. Online College Courses
3. Personal email through Yahoo, Gmail, Live.com, and others.
4. Online purchases for classroom and home

FAQ Non-acceptable uses:

1. Streaming audio and video data is not allowed due to potential negative impact on network performance. If streaming sites are identified as educational, it might be possible to unblock those sites, but it isn't guaranteed depending upon the streaming network setup.
2. Selling or managing sales for personal business

Student Internet Access Filtering

Students are not permitted to be on social networking sites like Facebook, MySpace, etc.

Students should use Google or Yahoo search because safe filtering is forced. At this time, BING is not allowed to use as a search engine because it allows inappropriate content from a bad site to be sent from a BING search server as unfiltered.

Students are allowed to use personal email (Yahoo, Gmail, etc.). It is recommended that teachers use Gaggle.com for classroom email projects. Hillsboro R-3 has free enrollment in Gaggle.com email service and it provides full teacher monitoring of student email.

Students are allowed to use online games that are acceptable in content.

Students are allowed use network storage to save documents and classroom activity files like Powerpoints, Moviemaker, etc. It is not allowed to use network storage to save downloaded music, executable programs/games, etc.

Email and online gaming are completely at the discretion of the teacher. If you do not want your students accessing these sites, please make it a rule in your classroom.

The Student Internet Use Agreement states that students and/or their work may be recognized on the district's website in the form of lists or photos. Parents must request in writing if they want their child to be exempt from this policy.

Student Supervision and Monitoring on Internet Use:

It shall be the responsibility of all members of the Hillsboro R-3 School District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act. A TEACHER'S EYES ARE THE BEST FILTERING SYSTEM. Do not assume that our filtering is fail proof because if it can be found, our dedicated students will find it.

Employee Passwords

Any employee found to have violated this policy may be subject to disciplinary action, up to and including suspension of technology use, expulsion, termination of employment, civil and/or criminal penalties. If an employee chooses not to use a strong, protected password and security of sensitive information is compromised due to negligence, that employee will be held responsible for any damages.

Email and network log-in passwords should be strong with a mix of upper/lower case letters, numbers, and other special characters. It is recommended that a strong password be at least 15 characters.

Passwords should be changed at least once every year or sooner if that password is thought to be compromised.

Never use personal names, birthdates, pet names, nicknames, or anything else that is easily associated with you.

TECHNOLOGY RULES AND REGULATIONS

Email Use

Purpose:

To prevent tarnishing the public image of Hillsboro R-3 School District When email goes out from Hillsboro R-3 School District the general public will tend to view that message as an official policy statement from the Hillsboro R-3 School District.

Scope:

These rules and regulations covers appropriate use of any email sent from a Hillsboro R-3 School District email address and applies to all employees, vendors, and agents operating on behalf of Hillsboro R-3 School District.

Prohibited Use:

The Hillsboro R-3 School District email system shall not to be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any Hillsboro R-3 School District employee should report the matter to their supervisor immediately. District email system shall not be used for the purpose of personal financial gain (ex. Inviting individuals to a party for selling items, selling tickets to events, advertising a business, etc.).

Personal Use:

Using a reasonable amount of Hillsboro R-3 School District resources for personal emails is acceptable, but it is encouraged to use a personal email account (examples include Yahoo, Google, Hotmail, etc.). Sending chain letters or joke emails from a Hillsboro R-3 School District email account is prohibited. Virus or other malware warnings and mass emailing about non-school business within our school district and emails from Hillsboro R-3 School District shall be approved by Hillsboro R-3 School District Director of Technology or Superintendent before sending. These restrictions also apply to the forwarding of mail received by a Hillsboro R-3 School District employee.

Monitoring:

Hillsboro R-3 School District employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. Hillsboro R-3 School District may monitor messages without prior notice. Hillsboro R-3 School District is not obliged to monitor email messages.

Confidentiality Notice:

Hillsboro R-3 School District employees must include the Confidentiality Notice with all emails, internal and external. The Confidentiality Notice is a statement of unauthorized

disclosure meaning the intentional or unintentional revealing of restricted information to people, both inside and outside Hillsboro R-3 School District, who do not have a need to know that information. The confidentiality notice reads as provided below.

CONFIDENTIALITY NOTICE: If you have received this e-mail in error, please immediately notify the sender by e-mail at the address shown. This e-mail transmission may contain confidential, proprietary or privileged information and may be subject to protection under the law, including the Family Educational Rights and Privacy Act (FERPA) and/or the Health Insurance Portability and Accountability Act (HIPAA). This information is intended only for the use of the individual(s) or entity to who it is intended even if addressed incorrectly.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Email - The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.

Forwarded email - Email resent from an internal network to an outside point.

Chain email or letter - Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.

Sensitive information - Information is considered sensitive if it can be damaging to Hillsboro R-3 School District or its customers' reputation or market standing.

Virus warning. - Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.

Unauthorized Disclosure - The intentional or unintentional revealing of restricted information to people, both inside and outside Hillsboro R-3 School District, who do not have a need to know that information.

TECHNOLOGY RULES AND REGULATIONS

District Email Retention

Purpose:

The Email Retention Archive Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas that follow this introduction.

Questions about the proper classification of a specific piece of information should be addressed to your manager. Questions about these guidelines should be addressed to Hillsboro R-3 School District.

Scope:

This email retention archive policy is secondary to Hillsboro R-3 School District policy on Freedom of Information and Business Record Keeping. Any email that contains information in the scope of the Business Record Keeping policy should be treated in that manner. Individual departments are responsible for their legal responsibilities defined by the Missouri Department of Elementary and Secondary Education for retaining email as a part of student records.

Policy:

Email Archiving
Hillsboro R-3 District email will be archived for the period of one (1) year. All archives will be maintained on an email or archive server. Once a month archive has been retained more than 12 months, it will be deleted at the end of the 13th month of retention.

Recovering Deleted Email via Backup Media
Hillsboro R-3 School District maintains backup of archives on a backup server and the retention policy will be followed on this server as well.

Definitions:

Approved Electronic Mail
Includes all mail systems supported by the IT Support Team. These include, but are not necessarily limited to, Groupwise email. All district email should be conducted on the district's approved email system. Personal email should not be used to conduct school business without prior approval by administrators in the Technology Department or Administration office.

Approved Instant Messenger

The Groupwise IM Client is the only IM that is approved for use on Hillsboro R-3 School District computers.

Individual Access Controls
Individual Access Controls are methods of electronically protecting files from being accessed by people other than those specifically designated by the owner. On UNIX machines, this is accomplished by careful use of the chmod command (use *man chmod* to find out more about it). On Mac's and PC's, this includes using passwords on screensavers, such as Disklock.

Insecure Internet Links
Insecure Internet Links are all network links that originate from a locale or travel over lines that are not totally under the control of Hillsboro R-3 School District.

TECHNOLOGY RULES AND REGULATIONS

Internet Safety

Introduction:

It is the policy of Hillsboro R-3 School District to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Definitions:

Key terms are as defined in the Children's Internet Protection Act.

Access to Inappropriate Material:

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors. Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Inappropriate Network Usage:

To the extent practical, steps shall be taken to promote the safety and security of users of the Hillsboro R-3 School District online computer network when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.
Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes: (a) unauthorized access, including so-called 'hacking,' and other unlawful activities; and (b) unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

Supervision and Monitoring:

It shall be the responsibility of all members of the Hillsboro R-3 School District staff to supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of director of technology or designated representatives.

Adoption:

The Board of Hillsboro R-3 School District adopted this Internet Safety Policy at a public meeting, following normal public notice, on July 23, 2009.

CIPA definitions of terms:

TECHNOLOGY PROTECTION MEASURE. The term “technology protection measure” means a specific technology that blocks or filters Internet access to visual depictions that are:

1. **OBSCENE**, as that term is defined in section 1460 of title 18, United States Code;

2. **CHILD PORNOGRAPHY**, as that term is defined in section 2256 of title 18, United States Code; or

3. Harmful to minors.
HARMFUL TO MINORS. 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;
>
> 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 as to minors.
> **SEXUAL ACT; SEXUAL CONTACT.** The terms “sexual act” and “sexual contact” have the meanings given such terms in section 2246 of title 18, United States Code.

TECHNOLOGY RULES AND REGULATIONS

Electronic Devices

Students

OTHER ELECTRONIC DEVICES

Student's personal electronic devices (i.e. iPods, MP3 players, laptops, tablets, etc.) may be used during the instructional day in accordance with classroom rules and procedures. Personal laptops and wireless devices are allowed to only connect to the district's wireless guest network (filtered according to CIPA - Federal Children's Internet Protection Act guidelines). The district will provide the wireless guest network for connectivity, but it is the responsibility of users (students) to maintain and administer their personal devices' ability to connect. The wireless guest network is provided as a privileged resource to connect to the Internet and district's publicly accessible servers (i.e. district web server, district email, student information server, etc.). CIPA guidelines are to be followed while the personal wireless device is being used on campus. Student use of personal electronic devices is always subject to the school building policies.

The District is not responsible for lost, stolen, or damaged electronic communication devices or any charges incurred as a result.

Faculty, Staff, and Administration

CELL PHONE POLICY

Use of devices on school grounds – Electronic communication devices may be used before and after the instructional day, planning period, during lunch, and other times as deemed appropriate by buildings

OTHER ELECTRONIC DEVICES

Personal laptops and wireless devices are allowed to only connect to the district's wireless guest network (filtered according to CIPA - Federal Children's Internet Protection Act guidelines). The district will provide the wireless guest network for connectivity, but it is the responsibility of users to maintain and administer their personal devices' ability to connect. The

wireless guest network is provided as a privileged resource to connect to the Internet and district's publicly accessible servers (i.e. district web server, district email, student information server, etc.). CIPA guidelines are to be followed while the personal wireless device is being used on campus. The use of personal electronic devices is subject to the school building policies.

The District is not responsible for lost, stolen, or damaged electronic communication devices or any charges incurred as a result.

TECHNOLOGY RULES AND REGULATIONS

Cyber Bullying

Purpose:

Hillsboro R-3 School District strives to provide a safe, positive learning climate for students in the schools. Therefore, it shall be the intent of the School District to maintain an educational environment in which bullying and cyber bullying in any form are not tolerated.

All forms of cyber bullying by school district students are hereby prohibited. Anyone who engages in cyber bullying in violation of these rules and regulations shall be subject to appropriate discipline.

Students who have been cyber bullied shall promptly report such incidents to any staff member.

Complaints of cyber bullying shall be investigated promptly as felt necessary by building administrators, and corrective action shall be taken when a complaint is verified. Neither reprisals nor retaliation shall occur as a result of the submission of a complaint.

The School District shall annually inform students that cyber bullying of students will not be tolerated.

Definitions:

Cyber bullying includes, but is not limited to, the following misuses of technology: harassing, teasing, intimidating, threatening, or terrorizing another student or staff member by way of any technological tool, such as sending or posting inappropriate or derogatory email messages, instant messages, text messages, voicemail messages, digital pictures or images, or website postings (including blogs) which has the effect of:

1. Physically, emotionally or mentally harming a student;

2. Placing a student in reasonable fear of physical, emotional or mental harm;

3. Placing a student in reasonable fear of damage to or loss of personal property; or

4. Creating an intimidating or hostile environment that substantially interferes with a student's educational opportunities.

All forms of cyber bullying are unacceptable and, to the extent that such actions are disruptive of the educational process of the School District, offenders shall be subject to appropriate staff intervention, which may result in administrative discipline.

The term "cyber bullying" shall not be interpreted to infringe upon a student's right to engage in legally protected speech or conduct.

Delegation of Responsibility:

Each staff member shall be responsible to maintain an educational environment free of

cyber bullying.

Each student shall be responsible to respect the rights of his/her fellow students and to ensure an atmosphere free from all forms of cyber bullying.

Students shall be encouraged to report cyber bullying complaints to any staff member.

Any staff member who receives a cyber bullying complaint shall gather information or seek administrative assistance to determine if cyber bullying has occurred. If the behavior is found to meet the definition of cyber bullying, the building principal must complete the appropriate written documentation.

The building principal or his/her designee will inform the parents or guardians of the victim and also the parents or guardians of the accused.

Complaint Procedure:

A student shall report a complaint of cyber bullying, orally or in writing, to a staff member. If a parent initiates the complaint, the appropriate staff member will follow-up with the student.

The staff member will either gather the information or seek administrative assistance to determine if the alleged cyber bullying conduct occurred.

After the information has been gathered, the building principal shall be notified of the complaint. The building principal will determine the need for further investigation or the appropriate intervention, which may result in administrative discipline to ensure that the conduct ceases. If the behavior is found to meet the definition of cyber bullying, the building principal must complete the appropriate written documentation.

A violation of these rules and regulations shall subject the offending student to appropriate disciplinary action, consistent with the student discipline code, which may include suspension, expulsion or notification to the appropriate authorities.

TECHNOLOGY RULES AND REGULATIONS

Automated Communication System

Purpose:

Automated Communication System is a resource to be used for time-critical emergencies and announcements for employees (faculty, administration, staff, etc.), students, parents, and community (as related to school). (NOTE: Building level usage has some flexibility per principal approval; however it is strongly encouraged to use other means of communication when possible.)

The system will be utilized for school and event cancellations/closings, however, it is not considered the primary source. Local radio and television stations are considered the primary source for communicating closings and cancellations. School and event cancellations/closings will be posted on the district's website as well.

General announcements may be made through the system as well, but recommended only if other methods of communication (flyers, letters, etc.) were not possible due to means other than poor planning.

Message length is recommended not to exceed more than one minute.

The system effectiveness is defined by its primary use for emergencies and time-critical announcements.

TECHNOLOGY RULES AND REGULATIONS

Password Use

Overview:

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Hillsboro R-3 School District's entire network. As such, all Hillsboro R-3 School District employees (including contractors and vendors with access to Hillsboro R-3 School District systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose:

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope:

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Hillsboro R-3 School District facility, has access to the Hillsboro R-3 School District network, or stores any non-public Hillsboro R-3 School District information.

General:

· All system-level passwords (e.g., root, enable, network admin, application administration accounts, etc.) should be changed on at least an annual basis or sooner if the password security has been compromised.

· All user-level passwords (e.g., email, web, desktop computer, etc.) should be changed at least every year or sooner if the password security has been compromised.

· User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

· Passwords must not be inserted into email messages or other forms of electronic communication. This does not apply to temporary passwords used to initially setup accounts.

· All user-level and system-level passwords must conform to the guidelines described below.

Guidelines:

A. General Password Construction Guidelines

Passwords are used for various purposes at Hillsboro R-3 School District. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password (4 numbers only), and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than 8-10 characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:

    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words "Hillsboro R-3 School District", "sanjose", "sanfran", “hawks”, or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least fifteen alphanumeric characters long and is a passphrase (**Ohmy1stubbedmyt0e**?).
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "**TmB1w2R**?!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

It is not recommended to use the same password for Hillsboro R-3 School District accounts as for other non-Hillsboro R-3 School District access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various Hillsboro R-3 School District access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for a network account.

Do not share Hillsboro R-3 School District passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Hillsboro R-3 School District information.

Here is a list of "dont's" that are strongly encouraged:

· Don't reveal a password over the phone to ANYONE

· Don't reveal a password in an email message

· Don't reveal a password to the boss

· Don't talk about a password in front of others

· Don't hint at the format of a password (e.g., "my family name")

· Don't reveal a password on questionnaires or security forms

· Don't share a password with family members

· Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

It is strongly recommended to not use the "Remember Password" feature of applications.

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every year.

Enforcement:

Any employee found to have violated this policy may be subject to disciplinary action, up to and including suspension of technology use, expulsion, termination of employment, civil and/or criminal penalties. If an employee chooses not to use a strong, protected password and security of sensitive information is compromised due to negligence, that employee will be held responsible for any damages.

Definitions:

Terms Definitions

Application Administration Account Any account that is for the administration of an application (e.g., database administrator, network administrator).