Technology
Rules and Regulations

Hillsboro R-3 School District
Technology Department

Original Issue Date: 07/23/2009
Revised Date: 02/06/2009

Table of Contents

Email

Email sent from the Hillsboro R-3 School District will tend to be viewed as an official statement from the district. The rules and regulations listed below cover appropriate use of email sent from the Hillsboro R-3 School District and applies to all employees, students, vendors, and agents operating on behalf of the Hillsboro R-3 School District.

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.

Anyone with access to a Hillsboro R-3 School District email account shall have no expectation of privacy in anything they store, send or receive on the District's email system. Hillsboro R-3 School District may monitor messages without prior notice, but is not obligated to do so.

Email Retention Policy

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.

Effective July 1, 2015, the Hillsboro R-3 School District email will be archived indefinitely.

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, Microsoft, etc.).

- 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 and Superintendent before sending.

Confidentiality Statement

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.

Personal Electronic Devices

Personal electronic devices are permissible, such as, laptops and wireless devices. However, personal devices are only allowed to 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 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.

Content Filtering and Monitoring

The district will monitor the online activities of students, staff, and anyone using district resources by operating a technology protection measure ("content filter") on the network and all district technology with Internet access, as required by law. In accordance with law, the content filter will be used to protect against access to visual depictions that are obscene or harmful to minors or are child pornography. Content filters are not foolproof, and the district cannot guarantee that users will never be able to access offensive materials using district equipment. Evading or disabling, or attempting to evade or disable, a content filter installed by the district is prohibited.

The superintendent, designee or the district's technology administrator may fully or partially disable the district's content filter to enable access for an adult for bona fide research or other lawful purposes. In making decisions to fully or partially disable the district's content filter, the administrator shall consider whether the use will serve a legitimate educational purpose or otherwise benefit the district.

The superintendent or designee will create a procedure that allows students, employees or other users to request that the district review or adjust the content filter to allow access to a website or specific content.

Student Internet Filtering

Students are not permitted to be on social networking sites like Facebook, Snapchat, Instagram, etc. Students are allowed to use network storage to save documents and classroom activity files like PowerPoint presentations, Moviemaker, etc. However, students are not allowed to use network storage to save downloaded music, executable programs/games, etc.

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.

Cyber Bullying

The 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:

- Physically, emotionally or mentally harming a student;
- Placing a student in reasonable fear of physical, emotional or mental harm;
- Placing a student in reasonable fear of damage to or loss of personal property; or
- 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.

Employee Passwords Best Practices

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.

If an employee shares their password or 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.

Consequences

Any employee or student found to have violated the District technology policy and/or procedures may be subject to disciplinary action, up to and including suspension of technology use, expulsion, termination of employment, civil and/or criminal penalties.