



# Internet Safety Guidelines for Staff and Students

The Hays Consolidated Independent School District provides technology resources to its students and staff for educational and administrative purposes. The goal in providing these resources is to promote educational excellence in the schools by facilitating resource sharing, innovation and communication with the support and supervision of parents, teachers, and support staff. The use of these technology resources is a privilege, not a right.

Proper behavior, as it relates to the use of computers, is no different than proper behavior in all other aspects of Hays CISD activities. All users are expected to use the computers and computer networks in a responsible, ethical, and polite manner. This document is intended to clarify provisions and procedures in place to address staff and student internet safety as required by the Children's Internet Protection Act (CIPA), Neighborhood Children's Internet Protection Act (NCIPA) and The Protecting Children in the 21<sup>st</sup> Century Act.

1. Control student and staff access to inappropriate materials, on the Internet and the World Wide Web;
  - District Internet Filtering (Technology Protection Measure) blocks access to at least, but not limited to the three categories of visual depictions specified by CIPA – obscene, child pornography, and harmful to minors
    - A staff member can request access to a specific URL for bona fide research or other lawful purpose via a technology workorder. All requests will be reviewed by the Executive Director of Technology or an appointed designee.
    - Students may have a less or more restrictive filter depending on their age group.
  - Supervision or monitoring of online activities
  - Educate students and staff on proper procedure for:
    - An inappropriate or harmful site coming up on the screen
      - Student:
        - Turn off monitor
        - Raise your hand
        - Wait for an adult to address the problem
      - Staff:
        - Turn off monitor and/or close browser
        - Report to Instructional Technology Specialist via a workorder
        - Request site to be blocked
    - Searching for information on the Internet
      - Do not type specific web address (if uncertain of the site address)
      - Use search engines when looking for specific sites
    - Create and use link pages for Internet access when appropriate
2. Ensure student safety and security when using online communications tools (OCT) such as email, chat rooms, and / or blogs;
  - Students are not to enter an electronic chat or any online communication tool without adult supervision.
    - Stress that no one ever knows for sure who is in the chat room watching or with whom he or she is communicating.
    - Educate students on online dangers
      - Compare stranger danger in cyberspace to the real world stranger danger.
      - Compare bullying in the real world to cyberbullying.
      - Discuss identity theft awareness.
  - Student personal email is not to be accessed at school without adult permission.
  - If a student needs to send an email for school use, a school email account such as the teachers or a special arranged class account can be used. (District email can be monitored.)

- Students should not access personal online communication tools such as but not limited to social networking sites such as Facebook, MySpace, Twitter etc. and/ or personal blogs and wikis at school. Exceptions will be made for lessons containing specific educational objectives and technology designee approval.

Personal online communication tool awareness:

- Manage your privacy settings such as directory information, invites, etc.
- Limit use of personal identifiable information on such sites.
- Be aware of your connections, people may not be whom they seem.
- Be aware of your “cyberspace” surroundings, you don’t know who else may be on that site.
- Once information is posted, it can live forever.
- Online choices can have offline consequences.
- Never agree to meet someone “offline.”
- Report any unlawful or inappropriate actions to authorities.
- Educational online communication tools may be accessed with adult supervision and implementation of the below guidelines.

Online communication tool guidelines:

- Instructional blogs and other online communication tools maintained by Hays CISD teachers must be hosted on an approved educational website.
- All instructional activities using blogs must be teacher moderated.
- Only private, monitored wikis are approved for use in the K-12 classrooms.
- Teachers should partner with their school Librarian or Instructional Technologist for projects utilizing OCT.
- To ensure safety of our students, the OCT moderator will:
  - Verify that the content relates to the instructional objective.
  - Verify that the content does not contain inappropriate language.
  - Verify that the content does not include identifying information such as a student’s full name, school name, city name, teacher’s name, phone number, address, etc. Examples of how students may sign an online posting include:
    - 4th Grader (non identifiable)
    - Josh L. (first name only, last initial only)
    - bookworm (alias)
  - If a student’s content in a project utilizing OCT includes an attachment such as a student produced project, photograph, or audio/video recording, the teacher must verify that appropriate parental consent is on file.
- Teachers will provide written communication to parents explaining how OCT will be used for instruction. Parents will be given an opportunity to decline participation for their child. A sample letter is available from the Hays CISD Technology Department.
- Prior to students utilizing OCT, the teacher must complete an Internet safety lesson provided by the Instructional Technologist with the participating students.

3. Prevent student and staff from unauthorized access, including “hacking,” and other unlawful activities;

- Personal Network Logins (Staff, Secondary and 5th grade Students)
  - Staff and students will be given specific rights based on their network login.
  - Staff and students are not to share their login or passwords.
  - Online activities may be monitored.
  - Activity on the network can be traced by the user’s login.
- Software installs disallowed at the user level.
- Virus Software installed on each desktop.
- Network measures in place to have a secure system.
- Copyright Laws / Proper Citing of Sites discussed.
- Personal Electronic Documents
  - Ownership of documents created.
  - Respect others’ documents.
  - Online documents may be monitored by administration.

4. Restrict unauthorized disclosure, use, and dissemination of personally identifiable information regarding students.
  - Student's full name, first and last, can be posted on the Internet as long as parental / guardian signed consent has been obtained and is on file.
  - Identifiable pictures of students can be posted to the Internet as long as parental / guardian signed consent has been obtained and is on file.
  - Students should not give out personal information over the Internet such as:
    - Name
    - Address
    - Phone Number
    - Age
  - Students should not share information that could identify him or her.
    - Landmarks about where one lives
    - Where one goes to school
    - Where one "hangs out"
    - Where parents work
    - Similar information about friends or family
  - Do not fill out forms on the Internet without parent or adult supervision. (Ex. membership forms, prize drawings, etc.)
  - If someone on the Internet asks you for personal information, turn off the monitor, raise your hand, and wait on an adult for assistance.
  - Never agree to meet someone "offline."
5. Measures designed to restrict minors' access to harmful materials on the Internet or World Wide Web. (See #1 for specifics.)

#### **Education, Supervision, and Monitoring:**

It shall be the responsibility of all members of the Hays CISD staff to educate, supervise, and monitor appropriate usage of the online computer network and access to the Internet in accordance with these guidelines, the CIPA, NCIPA, and the Protecting Children in the 21<sup>st</sup> Century Act.

#### **Internet Safety Sites:**

<http://www.cybersmart.org/home/>

[http://disney.go.com/legal/internet\\_safety.html](http://disney.go.com/legal/internet_safety.html)

<http://kids.getnetwise.org/safetyguide/>

<http://www.netsmartz.org/>

<http://www.oag.state.tx.us/criminal/cybersafety.shtml>

<http://www.safekids.com/>

<http://www.isafe.org>

This Internet Safety Guidelines document was presented to the Hays CISD District Leadership Team at their meeting, following normal public notice, on May 27, 2009.