Acceptable Use Policy

HAZLEHURST CITY SCHOOL DISTRICT	Policy Code: IFBGA
COMPUTER ACCEPTABLE USE POLICY	Adopted: July 2014

The Hazlehurst City School District (HCSD) offers currently enrolled students, faculty and staff access to the school computer network through computer labs, networked and stand-alone computers. District technology equipment is provided for use in fulfilling curriculum objectives and quality enrichment activities. Personal electronic devices are not to be connected to the District network. This includes, but is not limited to personal computers, laptops, tablets, smart phones, and MP3 Players.

The HCSD is in compliance with the Children's Internet Protection Act (CIPA) and will comply with any additional state and federal regulations that pertain to technology use within the district and through use of the HCSD network infrastructure and servers that is forthcoming from the local, state and federal regulatory agencies.

The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access in schools and libraries to the Internet and other information. Among many other things, it calls for schools and libraries to have in place appropriate electronic filters to prevent children and adults from accessing and viewing inappropriate Internet content. For any school or library that receives discounts for Internet access or for internal connections, CIPA imposes certain requirements. The HCSD receives these discounts for Internet Access through the E-Rate program and is therefore must be in compliance with CIPA.

COMPUTER NETWORK AND INTERNET USE RULES

Students and school personnel are responsible for good behavior on the school computer networks just as they are in a classroom or in a school hallway. Communications on the network are often public in nature. General school rules for behavior and communications apply. Within reason, freedom of speech and access to information will be honored.

In compliance with CIPA 2008 updates, all students (PreK-12) will be educated about appropriate online behavior, including interacting with other individuals on social networking websites, in chat rooms and in cyberbullying awareness and response. When using the Internet, all students will be closely monitored to prevent students from accidentally or otherwise accessing inappropriate material.

Computer access is a privilege, not a right, and is provided for students and staff to conduct research, fulfill course requirements, and communicate with others when appropriate or authorized. Access to network services is given to students and staff who agree to act in a considerate and responsible manner. Signed parental permission is required for all students. All faculty and staff using the district's Internet access must sign a written contract.

Network administrators may review network storage files and communications to maintain system integrity and ensure that users are using the system responsibility. While user files will not be examined without good cause, users should not expect that files stored on school computers will always be private. The HCSD will fully cooperate with local, state or federal officials in any investigation related to illegal activities conducted through any HCSD Internet account.

All users are expected to abide by the generally accepted rules of Netiquette. These include (but are not limited to) the following:

- Be polite. Do not be abusive or be "bullying" in your messages to others.
- Use appropriate language.
- Do not assume that email is secure and/or confidential. Never send anything that you would hesitate to have viewed by others.
- Respect other people's privacy regarding mail and files. Do not reveal personal address or phone numbers, or those of students or colleagues.
- Keep paragraphs short and to the point. Be mindful of spelling.
- Check email regularly and delete unwanted messages as quickly as possible.

NETWORK SECURITY – CIPA COMPLIANCE

Users have the responsibility to use computer and network resources for academic purposes only. Therefore, as mandated by CIPA, filtering and monitoring will be utilized on all computers accessing the Internet. Faculty and staff must use District provided email. Activities using the computer network in violation of Local, State, Federal or HCSD policies are strictly forbidden.

Students will not respond to unsolicited online contacts or reveal personal identifiable information over the network unless it meets District-approval (examples: ACT Registration,

Scholarships or College Applications). This includes information about themselves as well as information about anyone else.

HCSD staff is prohibited from disclosing personal information about students on websites. Although teachers and other district personnel may reveal personal information about themselves over the network, they are strictly forbidden to disseminate any student information electronically to any source that has not met district approval. Information that is considered personal includes but is not limited to the following: student's full name, home address, Social Security number, personal telephone numbers, and any information relating to their health.

Because there are additional prohibitions with which users must comply, non-compliance with these regulations will result in disciplinary and/or legal actions taken by the HCSD authorities if deemed necessary.

There is absolutely no expectation of privacy on the HCSD network. Activities at any workstation or transmission and receipt of data can be monitored at anytime both electronically or by staff members. This includes the transmission and receipt of email, email attachments, Web browsing and any other use of the network.

Prohibited activities include, but are not limited to the following:

- Using the network to transmit, or retransmit copyrighted material (including plagiarism).
- Accessing, transmitting, or retransmitting threatening, harassing, bullying (cyberbullying) obscene and pornographic or trade secret material or any material deemed harmful to minors.
- Using the network to access, transmit or retransmit language that can be considered defamatory, abusive or offensive.
- Using social networking sites, chatting, or blogging unless associated with a specific curriculum related activity.
- Users of the HCSD network are forbidden to access, transmit, or retransmit information that could cause danger or disruption, engage them in personal, prejudicial or discriminatory attacks or that harasses or causes distress to another person.
- Users of the district network are forbidden to access transmit, or retransmit material that promotes violence or the destruction of persons or property by any device including but not limited to firearms, explosives, fireworks, smoke bombs, incendiary devices or other similar material.

- All users agree to report any accidental access of any of the aforementioned material to the appropriate school authority so that the district can take steps to prevent similar future access.
- Using the network to download, upload or store large files such as music and video that are not directly related to projects or activities that are a part of the school curriculum.
- The use of flash (thumb) drives is limited to data storage only.
- No executable files of any type may be transferred to district property.
- Re-sending email chain letters or engaging in any spamming activities where bulk mailings of unsolicited email are sent.
- Damaging computers, computer systems, or computer networks (hardware or software). If a student maliciously damages HCSD technical equipment in such a way that requires service or repairs, the parent/guardian of the student is responsible for providing all expenses incurred for those services, grades PreK-12.
- Deliberate or careless action that damages the computer's configuration or limits the computer's usefulness to others.
- Downloading unauthorized software on school computers/networks. This includes students, teachers, staff and administrators. All software installed on district computers must be installed by the Technology Department and only after the proper licenses or authorizations for use have been acquired and verified.
- Creating, uploading, or transmitting computer viruses, worms or other disruptive software code.
- Making any attempt to defeat computer or network security on the district network or any other client, server, or network on the Internet. Hacking or attempting to gain access to unauthorized areas of the district network or the Internet is prohibited.
- Invading the privacy of other individuals. Using another person's password or account or providing his/her password to another person. Trespassing in another's folder, work or files, in the attempt to use others' work to "cheat" on assignments, tests, or any class work.
- Intentionally wasting limited resources.
- Using the network or school computer for unauthorized commercial, private, personal purposes or political lobbying.
- Any activity harmful to or reflecting negatively on the HCSD community.

CONSEQUENCES OF POLICY NON-COMPLIANCE

Violation of this AUP (Acceptable Use Policy) may result in the denial, suspension or cancellation of the users' privileges as well as other disciplinary and/or legal action deemed appropriate and imposed by the school administration, district administration and/or local, state or federal law enforcement officials.