STAFF INTERNET SAFETY POLICY

Definitions

TERM	DEFINITION
AUP	The term, **"AUP"** is defined as the Acceptable Use Policy of the District, attached hereto, incorporated herein, and made a part hereof for all purposes.
CIPA	The term **"CIPA"** is defined as the Children's Internet Protection Act (Pub. L. 106-554).
District	The term, **"District"** is defined as John H. Wood, Jr. Public Charter District.
Employee	The term, **"Employee"** or **"Employees"** refers to a person or to persons currently or previously employed by the District.
Student	The term, **"Student"** or **"Students"** refers to a person or to persons currently or previously enrolled in the District.
Network	The term, **"Network"** is defined as the electronic communications system of the District, including but not limited to the Intranet Network, E-Mail, and the World Wide Web (Internet).
Staff ISP	The term, **"Staff ISP"** is defined as this Staff Internet Safety Policy.

Purpose

The District has implemented the Network to provide safe, secure, effective, and efficient electronic communication for its Employees. It is the policy of the District to (1) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail ("E-Mail"), or other forms of electronic communications; (2) prevent unauthorized access and other unlawful online activity; (3) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (4) comply with CIPA.

The District has technology protection measures for all networked computing devices in the District that block and/or filter visual depictions that are obscene, pornographic, and harmful to minors as defined in CIPA. The school district will certify that schools in the district including media centers and libraries are in compliance with CIPA.

Compliance measures contained within this policy address the following:

Acceptable Use

Access to the Network is a privilege, not a right. By executing this Staff ISP and the attached AUP, Employees certify their understanding of and their agreement to follow the district acceptable use policies and procedures.

Disclaimer of Liability

The District shall not be liable for Employees' inappropriate use of the Network, the violation of any local, state, or federal laws by Employees, Employee negligence or mistakes, and costs incurred by Employees.

Intellectual Property

Employees must comply with all software licenses, copyrights, and all other state and federal laws governing intellectual property and online activity.

Employees shall have limited rights to work they create using the District's electronic communications system. The District shall retain the right to use any product created in the scope of a person's employment even when the author is no longer an Employee of the District.

Monitored Use

Employees waive the right to privacy in anything they create, store, send, or receive on the Network. Designated district staff will be authorized to monitor Employee activity over the Network at any time to ensure appropriate use.

Electronic Communications

The E-Mail system is the property of the District. It has been provided by the District for use in conducting District business. All communications and information transmitted by, received from, or stored in this system are District records and property of the District. The E-Mail system is to be used for District purposes. Use of the Network for personal purposes is limited. Any electronic communications transmitted using or across the Network shall be in accordance with district acceptable use policies and procedures.

Employees have no right of personal privacy in any matter stored in, created, received, or sent over the E-Mail system or any other District electronic systems.

The District, in its discretion as owner of the E-Mail system and any other electronic systems, reserves and may exercise the right to monitor, access, retrieve, and delete any matter stored in, created, received, or sent over any District system, for any reason and without the permission of any Employee.

Use of passwords or other security measures does not in any way diminish the District's rights to access materials on its system, or create any privacy rights of Employees in the messages and files on the system. Any password used by Employees must be revealed to the District as electronic files or E-Mail may need to be accessed by the District in an Employee's absence.

Even though the District has the right to retrieve and read any electronic messages, those messages should still be treated as confidential by other Employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any electronic messages that are not sent to them. Any exception to this policy must receive the prior approval of the Superintendent.

The District E-mail retention policy is set at 30 days; E-mails are automatically deleted once they age beyond 30 days and it is the responsibility of Employees to backup E-mails necessary to perform their job functions appropriately and in accordance with local, state, and federal document retention policies.

Password Security

Users of the District's network must use passwords that are unique and not easily guessed. Passwords should not be easily accessible to others or stored near the computer. Password guidelines are as follows:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length

Contain characters from **three of the following four** categories:

- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)

Passwords are set to expire every six months usually around July and January.

Intranet

SharePoint is a web-based Intranet for sharing information, documents and reports across the district. All District forms can be found on SharePoint. The site also contains District announcements and opportunities for specific groups to discuss their professional work. The announcements will be passed down and passed up weekly. Student records are also stored at this site. All Employees must check this site daily.

Information, files, and applications shared across the Network must not be in violation of license agreements or state or federal copyright laws. Only legally obtained and approved files and applications may be placed on the Network. The Director of Technology must approve the uploading or installation of any applications onto the Network.

Virtual Private Network (VPN)

It is the responsibility of Employees with VPN privileges to ensure that unauthorized users are not allowed access to the District internal networks. The following requirements must be followed at all times in order to maintain VPN security and integrity:

- Authorized users must keep information accessed via VPN in complete confidence.
- All computers connected to the District's internal networks via VPN or any other technology must use the most up-to-date anti-virus software.
- Employees are prohibited from time stamping in and time stamping out from Kronos while on VPN.
- If an Employee believes the Network was compromised, please report any information to the Director of Technology immediately via E-mail or written statement.
- Users are required to follow technology policies and/or proper Employee conduct policies.
- Users are required to report any policy violations to the Director of Technology via E-mail or written statement
- Any Employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Technology Protection Measure (Internet Filtering)

The District has selected a technology protection measure (Internet filtering) for use with the Network. The filtering technology will always be configured to protect against access material that is obscene, illegal (e.g. child pornography) and material that is harmful to minors, as defined by CIPA. The District or individual schools may, from time to time, reconfigure the filtering software to best meet the educational needs of the district or schools and address the safety needs of the Employees.

The District technology department will conduct an annual analysis of the effectiveness of the selected filter and will make recommendations to the Superintendent regarding the selection and configuration of the filter.

The filter may not be disabled at any time that students may be using the Network, if such disabling will cease to protect against access to materials that are prohibited under CIPA. The filter may be disabled during non-student use time for system administrative purposes.

Filtering technology has been found to inappropriately block access to appropriate material. To ensure that the implementation of the technology protection measure is accomplished in a manner that retains District control over decision making regarding the appropriateness of material for Employees, that does not unduly restrict the educational use of the Network by teachers and students, and ensures the protection of students' constitutional right to access to information and ideas, authority will be granted to selected educators to temporarily or permanently unblock access to sites blocked by the filter.

Authority to temporarily unblock access may be granted to school administrators and or his/her designees, and any media specialists or teacher who regularly uses the Internet for instructional purposes who request permission to have such authority. Individuals granted authority to temporarily unblock sites must meet standards for technical proficiency that are deemed necessary to ensure the security of the system. The technology department shall determine such standards.

To temporarily unblock a site, the authorized individual must review the content of the site, outside of the presence of any Employee, prior to allowing access to the site by an Employee.

Reports of all instances of temporary unblocking will automatically be forwarded to the Director of Technology.

If an unauthorized individual believes that the blocked site should be permanently unblocked, a request should be forwarded to the Director of Technology. The Director of Technology will make a decision to permanently unblock access to the site or may delegate the decision to the District technology committee. A list of all sites that have been permanently unblocked, together with the rationale for making the decision to unblock the site will be forwarded on a monthly basis to the superintendent and the District technology office.

Access by Minors to Inappropriate Content on the Internet and World Wide Web

Access to information for all students on the web will generally be limited to prescreened sites that are closely supervised by the teacher. The following policies are in place regarding the access of inappropriate content:

1. Students will not use the Network to access material that is profane or obscene (e.g. pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (e.g. hate literature). Special exception may be made for hate literature if the purpose of such access is to conduct research AND the teacher and the parent / guardian approve access.

2. If a student inadvertently accesses such information, they should immediately notify their teacher. Teachers and staff should immediately notify the campus administration, who will immediately notify the Director of Technology. This will protect students against an allegation that they have intentionally violated the AUP.

3. The fact that the filtering technology has not protected against access to certain material shall not create the presumption that such material is appropriate for students to access. The fact that the filtering software has protected access to certain material shall not create the presumption that the material is inappropriate for students to access.

The board of trustees of the District has authorized the superintendent to provide student access to Network resources only in supervised environments and has taken steps to lock out objectionable areas to the extent possible, but potential dangers remain and will be remedied as they are discovered.

Appropriate Online Behavior (Cyberbullying)

Pursuant to the Protecting Children in the 21st Century Act, it is the District's intention to ensure a safe online environment and to protect its students from harmful online behavior and "cyberbullying" (defined as the use of electronic media to harass, harm, threaten, embarrass, humiliate, or otherwise attack or target a minor) Measures to prevent and remedy inappropriate and harmful online behavior towards, by, and among students include, but are not limited to:

1. Student education on proper online behavior and etiquette, including all electronic interactions on social networking sites and in chat rooms, particularly with regard to "cyberbullying."

2. Staff training on "cyberbullying" prevention and intervention.

Additionally, students and staff are required to report instances of "cyberbullying" and inappropriate behavior to (a) ensure that incidents are property recorded, investigated, and remedied in a timely manner; and (b) to educate future preventative measures.

Failure to Follow Policy

Employees agree to abide by all policies, regulations, and guidelines governing the use of the Network at all times. Violations of any of these policies, regulations, or guidelines may result in disciplinary action, including termination of employment. Violations of law may result in criminal prosecution in addition to District disciplinary action. For further clarification on District disciplinary policy in the event of Network violations, please refer to the "Violations of this Acceptable Use Policy" Section of the Acceptable Use Policy for the Electronic Communications Equipment/System and to Sections 4.10 ("E-mail, Internet and other Electronic Systems") and 4.19 ("Employee Conduct") of the John H. Wood, Jr. Public Charter District Employee Handbook.

EMPLOYEE'S AGREEMENT

Employee Name: _____
Position: _____ Campus: _____

I have read the John H Wood Jr. Public Charter District Staff Internet Safety Policy document. I agree to follow the rules contained in this policy. I understand that if I violate the rules my access can be terminated and I may face other disciplinary measures.

Employee Signature:_____

Date:_____