CHARTIERS-HOUSTON SCHOOL DISTRICT

Policy No.: 703

Section: PROPERTY

POLICY GUIDE

Title: USE OF INTERNET/CHARTIERS HOUSTON SCHOOL DISTRICT NETWORK BY EMPLOYEES

Adopted: 4/21/97

Revision Adopted: 10/15/03; 3/19/07; 6/18/12

POLICY NO. 703
USE OF INTERNET/CHARTIERS-HOUSTON SCHOOL DISTRICT NETWORK/ DISTRICT TECHNOLOGY BY EMPLOYEES AND OTHER AUTHORIZED USERS

1. PURPOSE

The technology and telecommunication resources available in the District represent a large capital investment by our communities. The Board intends that access to the Internet, the School District's network system, and other technology be made available to employees and other authorized users for legitimate and lawful educational purposes; considers the Internet to be like a "digital" library where employees and other authorized users are expected to be responsible and accountable for their actions in accessing resources and sharing them with students just as they are in a traditional library; and expects employees and other authorized users to act as the school's ambassador when accessing the Internet as they do when physically traveling outside the School District for School District purposes.

To this end the Board established ***Responsible Use Guidelines*** to ensure proper and ethical use; to provide consistent, responsible access management; to conform usage with current law; to define parameters for acceptable use; and to impress upon employees and other authorized users that inappropriate use may result in a serious penalty.

The following ***Responsible Use Guidelines (RUGs)*** apply to all employees and other authorized users when they access any Chartiers-Houston School District computer, network or internet connection, other computer equipment and/or communication services owned or leased by the District. Prior to accessing the Internet/School District network/technology, each employee and other potential users must sign the attached acknowledgment form, acknowledging that he/she is aware of these Responsible Use Guidelines and agrees to comply with the same. The original executed acknowledgment form shall be maintained in the personnel file of any authorized user who is an employee, and shall be maintained in the place and manner as the Superintendent or his designee shall direct for any other authorized user.

The following ***RUGs*** also cover all other devices and items provided by the District which are deemed to be "technology," to the extent that any or all of the ***RUGs*** may apply, based upon the capabilities of the specific technology at issue. Such technology includes, but is not limited to, printers and calculators.

The following ***RUGs*** govern all in-school use, as well as any cyber education program that may at any time be provided by the District which would require employees and/or other authorized users to access any computer equipment, network or internet connection, communication services, or technology provided by the District.

2. AUTHORITY

The Board delegates to the Superintendent authority to implement these ***Responsible Use Guidelines.***

RESPONSIBLE USE GUIDELINES (RUGs)

3. GUIDELINES

1. **Cooperation**

It is understood that cooperation is critical in the use of the Internet/District network/technology at the Chartiers-Houston School District. It is the goal of the use of the Internet/District network/technology to prepare students to become technologically literate in an increasingly technological world. It is understood that independent use by employees and/or other authorized users of the Internet/School District's network/technology may be necessary to attain such a goal, subject to procedures and standards for appropriate behavior and communication.

2. **Discipline**

Violations of these ***Responsible Use Guidelines*** may result in appropriate discipline and/or other consequences to employees and other authorized users, which could include loss of use privileges to access the Internet/School District network/technology for a defined period or permanently, and/or suspension/dismissal and/or criminal and/or civil or legal proceedings.

3. **Access**

Only those employees and other authorized users who receive training through the District, or demonstrate to the satisfaction of the District's Business Manager or designee that they are appropriately trained/knowledgeable concerning use of the system, and execute the attached Acknowledgment Form shall be authorized to use the Internet/School District's network.

4. **Use is a Privilege - User Accountability**

It is understood that the use of the Internet/School District network/technology is a privilege, not a right. The equipment, hardware software or communication services allowing access to the Internet/District Network are the property of and/or under the possession and control of the School District. Use shall be reserved to those employees and other authorized users who utilize the materials that are of "educational value" to the programs of the Chartiers-Houston School District or directly related to the operation of the schools or School District business and are related to performance of that employee's or other authorized user's duties. For the purposes of these Guidelines, "educational value" shall mean those areas of Internet/District network access/uses of technology that have a direct or indirect impact on the student educational program at the Chartiers-Houston School District, and which are in line with the Board-approved curriculum. The use of the Internet/School District network/technology for E-Mail to be remitted to friends, chatting, reading jokes, searching sport sites, farming out information on games, or other actions that are not directly or indirectly related to the school's curricula are not deemed to be of "educational value" and will not be permitted.

5. **Other Prohibited Uses**

The use of the system/technology for defamatory, inaccurate, obscene, profane, sexually oriented or threatening material, or

abusive or racially, ethnically, or religiously offensive material which is not of educational value in line with Board-approved curriculum, not a matter of public concern, and/or which causes or could reasonably cause disruption to the effective operation of the School District, or other illegal material shall also be prohibited and the Chartiers-Houston School District will use any and all efforts available to it, within the confines of the law, to prevent such material from entering the system.

In accordance with the Pennsylvania Child Internet Protection Act, use of any computer equipment and/or communications services owned or leased by the Chartiers Houston School District for sending, receiving, viewing or downloading visual depictions of obscenity, child pornography or material that is harmful to minors, as those terms are defined in the Act (24 P.S. section 4603) is prohibited. The District shall use Astaro filter/firewall software, and/or any and all other software, servers or other programs deemed appropriate by the District in the future to block access to any visual depictions prohibited under the Pennsylvania or federal Child Internet Protection Act.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the District's computers and other technology are being used for purposes prohibited by law or for accessing sexually explicit materials. These procedures shall include, but may not be limited to:

1. Using a technology protection measure that blocks or filters Internet access from users to certain visual depictions that are obscene, child pornography, material that is harmful to minors, or determined by the Board to be inappropriate for use by students.

2. Maintaining and securing a usage log.

3. Monitoring online usage of all users.

In addition, prohibited uses of the Internet/District Network/technology include, but are in no way limited to the following:

1. Violating any federal, state, or local criminal/civil statutes or ordinances, or facilitating illegal activity

2. Using the Internet/District network/technology for solicitation, commercial gain, gambling or profits

3. Transferring copyrighted and/or licensed materials to or from any District network or other item of District technology without the express consent of the owner of the copyright/license.

4. Performing non-school related work.

5. Advertising products or performing political lobbying.

6. Bullying.

7. Disseminating hate mail, discriminatory remarks, and defensive or inflammatory communication.

8. Installing, distributing, reproducing, or using copyrighted materials illegally or without authorization.

9. Accessing obscene or pornographic material or child pornography.

10. Accessing material that is harmful to minors or is determined to be inappropriate for students in accordance with Board policy.

11. Using inappropriate language or profanity.

12. Impersonating another user, or using the Internet or other technology anonymously or under pseudonyms.

13. Disrupting the work of other users.

14. Destroying, modifying, abusing, accessing, transferring, and/or copying, without authorization, any hardware, software, files, passwords and/or data belonging to the District or others.

15. Quoting of personal communication in a public forum without the original author's prior consent.

16. Attempting to circumvent the system security, guess passwords, gain unauthorized access to local or wide area network resources, or attempting to harm the system or infect it with a virus.

17. Attempting to circumvent security procedures to break into a file

18. Moving, repairing, reconfiguring, modifying, or attaching external devices to the computer/network without permission of the District Superintendent or his/her designee, reconfiguring, modifying or attaching external devices to the computer/network without permission of the District's Superintendent or his/her designee. This prohibition does not apply to use of thumb-drives or USB drives for school-related work.

19. Theft of any technology, or technology-related time or services.

20 Causing damage to any District technology in any other manner.

21. Any other misuse of technology for any purpose other than a use for which the technology is intended and an activity which has educational value, and is in line with Board-approved curriculum.

6. Review of Prohibited Uses

The Board is aware that due to the vastness of information on the Internet, situations may occur when these Responsible Use Guidelines or the blocking software or devices may prohibit access to material being sought for legitimate research of "educational value," directly related to a curricular project. If an employee or other authorized user reasonably believes that this Policy is denying him/her access to material that is not within the prohibition of these Responsible Use Guidelines, he/she may set forth in writing, to the Superintendent:

(a) the information he/she is seeking to retrieve or send, and, if applicable, the Internet site he/she wishes to access; and

(b) the reason for obtaining or sending that information.

The Superintendent shall inform the employee or other authorized user, based on his interpretation of this Policy, of his decision to allow or to deny access to the site, within five (5) school days of receipt of the written request. This decision shall be final.

If the Superintendent agrees that access should be allowed for legitimate bona fide research of "educational value" or other lawful purpose, and the information sought is inaccessible due to the blocking software/ devices, then the Superintendent may have the blocking software or device disabled temporarily to allow access ONLY TO THAT EMPLOYEE OR OTHER AUTHORIZED USER FOR THE PURPOSE DEEMED APPROPRIATE BY THE SUPERINTENDENT.

7. **Reporting Inappropriate Behavior**

Each employee and other authorized user shall be responsible for immediately reporting to the building principal all knowledge of prohibited uses of the Internet/District network/technology. Only those uses of the School District system which are of educational value and not inconsistent with this Policy are permitted.

8. **Potential Liability**

All employees and other authorized users using the Internet/School District network are charged with recognizing that E-Mail or network messages may contain thoughts, conclusions, and certain biased perceptions that were never intended for publication. There may be liability for defamation for spreading false and disparaging information about third parties, particularly comments on other employees and other authorized users, students, personnel applicants, or various vendors. Such discussions or use on the Internet/network is expressly prohibited.

The District shall not be responsible for any unauthorized charges or fees resulting from access to the internet/School District network.

9. **District Not Liable for Content**

The electronic information available to students, employees and other authorized users does not imply endorsement by the District of the content, nor does the District guarantee the accuracy of information received. The District shall not be responsible for any information that may be lost, damaged or unavailable when using the Internet/District network or other technology or for any information that is retrieved via the internet.

10. **Compliance with Relevant Laws**

No personnel or student information, which is protected by the Family Educational Rights and Privacy Act, and/or other applicable statutes, shall be disseminated through the Internet/District network or other technology. Prior to communication of any personally identifying information relating to a student or former student, by email, an employee or other authorized user MUST obtain the prior written consent of the student's parent or legal guardian (if the student is a minor), or of the student, if the student is age 18 or older, on the form attached hereto and incorporated herein as Exhibit "A" to this Policy. Other authorized users must follow any and all procedures as may be required by the District for securing the District's authorization to submit "Exhibit A" to a parent/guardian/student for signature.

11. **Protection of Confidentiality**

All users of the Internet/School District network must comply with applicable federal and state laws prohibiting the unauthorized interceptions or disclosure of E-Mail messages by third parties.

12. **No Privacy Rights**

Employees and other authorized users who use the Internet/School District network/technology are charged with recognizing that the District Administration does have the authority to intercept E-Mail messages of all users and that there will be no privacy right construed by the District to exist in the statements made in the network, or in any other use of the Internet/District network or technology. Users of the Internet/network are discouraged from storing extensive E-Mail messages; in fact, messages which are no longer useful or necessary should be eliminated daily and no message may be stored longer for more than fourteen (14) calendar days, unless such message constitutes a record subject to the District's Records Management Plan and its implementing regulations, or a litigation hold has been issued.

13. **System Security**

Employees and other authorized users shall not allow any other person to use their password or to share their account. It is the user's responsibility to protect E-Mail accounts from unauthorized use by changing passwords periodically and using passwords that are not easily guessed.

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to files. To protect the integrity of the system, the following guidelines shall be followed:

1. Employees and other authorized users shall not reveal their passwords to another individual.

2. Employees and other authorized users are not to use a computer that has been logged in under another employee and other authorized user's name.

3. Any user identified as a security risk, having a history of problems with other computer systems, and/or a history of misuse of the District's system or other technology may be denied access to the network and/or other technology.

14. **Equity of Use**

Time restrictions on use of the Internet/School District network/technology may be imposed by the Superintendent and/or his designee to ensure equity of use of District equipment, and/or avoid interference with the delivery of the district's educational program to students during the student day.

15. **Reduction of Cost**

From time to time, the District may encourage employees and other authorized users to use certain other informational sources in order to minimize costs.

16. **Monitoring for Educational Use**

The District Administration reserves the right to use electronic devices, cards, or any other means of monitoring the manner in which research is performed, Internet sites are visited, and any other use is made of the internet/District network/technology, to determine whether the employee or other authorized user is using the system or other technology for an appropriate educational purpose.

17. **Student Use**

Employees and other authorized users, to the extent applicable, shall use their best judgment and discretion in authorizing student

access and monitoring student use of the Internet/School District network/technology. In accordance with District Policy relating to Use of the Internet /School District's Network by Students, student users will be required to obtain a Driver's License for use of the Internet/District network from a faculty member.

18. **Safety**

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any employee or other authorized user who receives threatening or unwelcomed communications shall report such immediately to an Administrator. Network users shall not reveal personal information to other users on the network.

Any District computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software, as referenced in the section of this Policy entitled "Other Prohibited Uses".

Internet safety measures shall effectively address the following:

1. Control of access by minors to inappropriate matters on the Internet.

2. Safety and security of minors when using electronic mail, chatrooms, and other forms of direct electronic communications.

3. Prevention of unauthorized on-line access by minors, including "hacking" and other unlawful activities.

4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.

5. Restriction of students' access to materials harmful to minors.

19. **Responsible Internet Use**

The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated about appropriate online behavior, including:

1. Interacting with other individuals on social networking websites and in chat rooms

2. Cyberbullying awareness and response.

4. DISSEMINATION Student handbooks will contain a copy of this Policy and the attached consent forms.

Legal Authority

Pennsylvania Child Internet Protection Act, 24 P.S. Section 4601, et. seq
Federal Communications Act (as affected by the federal Child Internet Protection Act and federal Protecting Children in the 21st Century Act), 47 U.S. Code Section 254
47 C.F.R. Section 54.520

EMPLOYEE OR OTHER AUTHORIZED USER USE OF INTERNET/SCHOOL DISTRICT NETWORK/TECHNOLOGY

ACKNOWLEDGMENT FORM

I,_____an employee or other authorized user of the Internet/network/technology of the Chartiers-Houston School District, hereby acknowledge that I have read and am familiar with the Responsible Use Guidelines established by the School District for an employee's or other authorized user's use of the Internet/District network/technology at the School District, and agree to comply with said Responsible Use Guidelines. I have received training in such use through the District, or I have demonstrated to the satisfaction of the District's Business Manager or designee that I am appropriately trained/knowledgeable. I recognize and agree that the executed original of this Acknowledgment Form shall be maintained in my personnel file within the Chartiers-Houston School District if I am an employee of the District, or shall be maintained in the place and manner directed by the Superintendent, if I am an other authorized user.

Date:_____

Signature_____
Printed Name_____

CHARTIERS HOUSTON SCHOOL DISTRICT EMAIL PERMISSION FORM

I, _____, an adult individual, residing at
(Print Name)
_____, am the parent or legal guardian of _____, a student in grade _____ of the Chartiers Houston School District, attending _____ School. I hereby give my permission to have the individuals listed below transmit to me by electronic mail the following information regarding this student, with said information to be transmitted to the following e-mail address:

Parent's/Legal Guardian's E-Mail Address: _____

Names of persons authorized to transmit this information to the above-referenced e-mail address:

_____	_____
(Print Name)	(Print Position)
_____	_____
(Print Name)	(Print Position)
_____	_____
(Print Name)	(Print Position)

I further agree to advise the School District in writing of the revocation of this permission and/or of the change in the email address to which the identified documents or information is to be submitted.

Documents or information to be provided: (Please check the documents to which this consent form relates)

- ☐ (1) Attendance, information and records
- ☐ (2) Grades
- ☐ (3) Curriculum-based Test Results
- ☐ (4) Standardized Test Results
- ☐ (5) Disciplinary Information and Records
- ☐ (6) Other: Please specify _____

_____ _____
Signature of Parent or Legal Guardian Date

Received by:_____ at _____ Building on the _____ day of _____, 200___.

Exhibit "A"