Section:	**NH** - 3 **-Work Environment**
Title:	**Technology Acceptable** Use **Policy**
Number:	**Section3-G**
Status:	**Active**
Legal:	
Adopted:	**August2009**
Last Revised:	**November 2012**

POLICY DETAIL

G. TECHNOLOGY ACCEPTABLE USE POLICY

PURPOSE: These procedures define the responsibilities of New Horizons Regional Education Centers' employees, non-employees, volunteers, and students using the computers, tele-communications, network, IT or personal devises such as laptops and Internet resources provided by the Centers. Every authorized user is required to read and acknowledge these procedures by signing the appropriate use agreement form. Student forms will be filed in their school offices. All other user forms will be on file in the Human Resources Department.

SCOPE: All New Horizons Regional Education Centers (NHREC) employees, non-employees, volunteers and student use.

STATEMENT OF PROCEDURE: The use of the NHREC Computer System and Network by persons other than employees and students should consist of activities necessary to support the purpose, goals and mission of NHREC. The following, although not inclusive, define specific acceptable and unacceptable uses of the NHREC Computer System and Network.

1. Privacy

Communications over the NHREC Computer System and Network shall be considered public information and handled as such. The NHREC Computer System and Network authorized users must not have and shall have no expectation of privacy in their use of the Computer System. All information created, sent received, accessed, or stored in the NHREC Computer System and Network is subject to inspection and monitoring at any time as authorized by the Executive Director or designee and may occur without notice to users. The Technology Department may periodically review directories or messages to determine compliance with this policy for acceptable use. If unacceptable content or use is found, access privileges may be removed and the offender counseled at an appropriate level as outlined in Section 12, Violations and Penalties, of this procedure.

No recording, capture or live streaming (broadcast, video, photo, audio, etc.) using any means of technology of any New Horizons activity on campus or off campus may be made without prior written approval of that program's Administrator or the Director. Any such recording, capture or streaming shall remain the property of New Horizons Regional Education Center under the control of the Director. No release or publishing of such information can be made without prior written approval of the Director.

2. Security

Access is restricted to the NHREC Computer System and Network and is **limited to authorized users only.** Authorized users are responsible for their individual account information and should take all precautions to prevent others from accessing their account. Authorized users are prohibited from knowingly disclosing or modifying any assigned or entrusted access control to their account (such as:

log-in identifiers, passwords, terminal identifiers, user identifiers, digital certificates, Internet Protocol (IP) addresses, etc.) for any purpose other than those required to perform authorized NHREC functions. Authorized users may only access, modify or destroy files, data and resources for which they are authorized and that lie within the scope of their responsibilities, and only in accordance with Virginia Electronic Records Guidelines. Malicious destruction or modification of data or resources is prohibited. All NHREC employees should immediately notify their administrator, principal, manager or teacher if they have identified a possible security breach.

Authorized users will not attempt to go beyond their authorized access to the NHREC Computer System and Network. 1bis includes attempting to log into the NHREC Computer System and Network through another authorized user account or accessing or attempting to access another authorized user's file without authorization. Unauthorized access is illegal, even if only for the purpose of browsing.

Authorized users will not deliberately attempt to disrupt the NHREC Computer System and Network performance or destroy data by spreading computer viruses or by any other means.

At no time is a connection authorized to the NHREC Local Area Network via a non- NHREC Computer System and Network device expect those enrolled in an authorized Bring Your Own Device program. Enrollment requires the approval of that program's Director or Principal and the completion of the two additional BYOD forms. These forms must be received by the networking support department before use or connection of such devices is authorized.

3. Facsimile (Fax)

Fax machines are to be used by authorized users. These machines are not to be used for sending or receiving personal correspondence. Any sender of personal correspondence is to be notified by the receiver to cease transmitting personal correspondence. Any review, dissemination or use of the fax transmission by a person other than the addressee is prohibited. Students are not authorized to use NHREC fax machines unless permission has been granted by an NHREC employee.

4. Telephone Service

NHREC telephone service, to include landlines and cellular/wireless telephones, is to be used for calls regarding students and other school business. The use of the Centers' phones for personal business should be kept to a minimum. Please be advised that any employee using the phone for personal use or personal business still have no right to privacy and may be monitored and reviewed by NHREC staff.

If **it is necessary,** employees may place a long distance call using the school phone. If these calls are not for school business, callers must complete, at the time of the call, Appendix II: Long Distance Call Log to record each long distance business call.

Personal long distance calls at school are discouraged; however, should they become necessary staff should receive approval from the facility administrator.

5. Copyright

NHREC policy on copyright will govern the use of materials accessed through the Computer System. Because the extent of copyright protection of some information found on the Internet is unclear, users will make a standard practice of requesting permission from the holder of the work if their use of the material has the potential of being considered an infringement.
Teachers will instruct students to respect copyrights and to request permission when appropriate.

Users must not knowingly load onto the NHREC Computer System and Network or use commercial software in violation of its copyright and/or licensing agreement and will not perform downloads or installs without the authorization of the Technology Department.

6. NHREC Computer System and Network Software

Only division approved and provided software shall be loaded on the NHREC Computer System and Network. No software such as applications, games, freeware, demonstration software, and shareware shall be downloaded or installed on device in the NHREC Computer System and Network without written approval from Technology Support Services Staff.

7. NHREC Device Check-Out

NHREC may allow an employee to "check-out" a technology device. NHREC owned technology devices are for professional school purposes only and employees checking out a device must adhere to NHREC's Acceptable Use Policy. Any device that is checked-out by an employee must be returned in the same condition as received, minus normal wear due to usage. The employee is responsible for any damages to the device. If employment is terminated by either party and the technology device is not returned, NHREC will proceed with payroll deduction at a value it determines appropriate based upon purchase price and age of device. Upon check-out of the NHREC owned device, the employee must complete and sign the NHREC Technology Device Sign-Out Form which documents the above mentioned stipulations.

8. Academic Freedom, Selection of Material, Student Rights to Free Speech

Federal and State Laws on academic freedom and free speech will govern the use of the Internet. When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to course objectives. Teachers will preview materials and sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the site.

9. NHREC Websites

NHREC has established a Web site and Web pages that present information about the NHREC. The Executive Director will designate an administrator to be responsible for maintaining the division Web Site. The principals or their designee(s) are responsible for overseeing the development and content of their school's web site and for ensuring that published content is relevant to the department/school and complies with the AUP Policy.

New Horizons Employee Handbook policy on Discrimination and Harassment applies fully to the NHREC published Internet sites. Abusive, vulgar, harassing, threatening or otherwise inappropriate content will not be published on New Horizons owned Internet sites.

NHREC web sites will not post photographs of our student population without permission from a parent or legal guardian. Student forms will be filed in their school offices. All other user forms will be on file in the Human Resources Department.

NHREC websites will not contain direct links to pages that violate the AUP policy.

10. Electronic Mail (e-mail)

The NHREC e-mail system provides authorized users the capability of sending and receiving electronic communications between all schools and the central office in addition to electronic communications outside the Centers. Use of the e-mail system should pertain to school related business only.

Authorized users will check their e-mail frequently and delete unwanted messages promptly. E-mails required to be filed for extended periods of time should be archived to CD or electronically stored outside the e-mail system.

As normal policy, students are not granted access to e-mail however, for special projects and programs, students will be granted access to the e-mail system for the duration of the program or project. It is the program or project administrator's responsibility to ensure the e-mail system is not abused or used in a matter other than described in the AUP for such programs and projects.

E-mails are written records and may be subject to inspection and monitoring as authorized by the Executive Director or designee and without notice to the user. Users must not have and shall have no expectation of privacy in e-mail. In addition, disclosure may occur pursuant to the Virginia Freedom of Information Act (FIOA), Code of Virginia, §2.2-3700 et seq., legal process and civil discovery, and division reviews and maintenance. The following are examples of inappropriate uses:

- Authorized users will not engage in spamming.
- Authorized users will not use the e-mail systems for personal gain, commercial purposes, or political lobbying.
- Authorized users will not use **personal** Face book or other publications seminar thereof.
- It is prohibited to use e-mail for the propagation of viruses, computer worms, Trojan Horses, and other malicious software acts.
- Authorized users will not engage in phishing.
- Authorized users will not transmit threatening, abusive, vulgar, obscene, or harassing e-mails.
- It is prohibited to attempt to subscribe an authorized user to any electronic mailing lists.
- With the exception of the NHREC web based e-mail system it is prohibited to access any web based e-mail system from any NHREC Computer System and Network.
- Any video or audio recordings of students and faculty during instructional hours will be considered NHREC property and can be confiscated even if done so with personal devices.

11. Text Messaging

Text messaging may be provided to those authorized users requiring cellular service as part of the job requirements for NHREC. Text messaging is not provided by default on a NHREC provided cellular device. Use of text-messaging should pertain to school related business only.

Authorized users must request that text messaging service be turned on for their approved cellular device and provide justification for its use in the performance of the users duties.

Text messages are written records and may be subject to inspection and monitoring without notice to the user. Users must not have and shall have no expectation of privacy in text messaging. In addition, disclosure may occur pursuant to the Virginia Freedom of Information Act (FIOA), Code of Virginia, §2.2-3700 et seq., legal process and civil discovery, and division reviews and maintenance.

12. Internet Safety and Ethics

The NHREC Computer System and Network will not be used to send, receive, view or download illegal/undesirable content/materials or to conduct illegal activities (e.g. arranging for the sale/purchase of drugs, engaging in criminal gang activity, pornography or threatening the safety of another individual). It is prohibited to use electronic communication services for fraudulent, threatening,

obscene, rude, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages. In addition, the NHREC Computer System and Network will not be used for commercial purposes, personal gain, or political lobbying.

Restrictions against inappropriate language apply to public messages, private messages and material posted on Web pages. Authorized users will conduct themselves in a manner that is appropriate and proper as representatives of the Centers.

Authorized users will subscribe only to discussion group mail lists that are Centers' sponsored/authorized, affiliated and/or relevant to school business. Authorized users will not access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). For students, a special exception may be made for hate literature only if the purpose of such access is to conduct research and access is approved both by the teacher and the parents or legal guardian.

The Children's Internet Protection Act (CIPA) requires schools and libraries rece1vmg E-Rate discounts for Internet access and internal connections to comply with the CIPA. NHREC has implemented an Internet Filter to block access to text and visual depictions deemed obscene, child pornography, or harmful to minors."

Internet filters are not fail-proof and therefore may not block all undesirable Web pages. Therefore, authorized users will only be allowed access to the Internet to pursue education-related activities. Teachers must keep up-to-date on Internet safety issues and provide accurate, timely information to students. Teachers will establish and post rules for safe Internet use near computers in classrooms, libraries and labs and remind students regularly that the rules are intended to ensure safety. Teachers should immediately notify an administrator, principal or Technology Department if they have identified a possible CIPA issue.

Authorized users will not post personal contact information about themselves or other people. Personal contact information includes school or work addresses, telephone numbers, etc. Students will not agree to meet with someone they have met online without the approval of their parents or legal guardians.

13. Violations and Penalties

Authorized users will be given notice of violations and given an opportunity to provide explanation for determination regarding continuing access to the NHR.EC Computer System and Network. Privileges may be suspended immediately. For employees, disciplinary action may be taken. Violations of the law will be reported to law enforcement officials. NHR.EC will cooperate fully with local, state, and federal officials in any investigation related to illegal activities conducted using the NHR.EC Computer System and Network.

Disciplinary action related to student access to electronic resources may be determined at the building and/or classroom level in accordance with existing policies and procedures as stated in NHREC's Policy, Student Rights and Responsibilities policy, and/or other Centers Policies and Procedures governing student discipline. Disciplinary actions should be tailored to assist the student in gaining the self-discipline to behave appropriately on an electronic network.

14. Definitions

- **Non-employees:** Contractors and support personnel who directly support the goals and mission ofNHR.EC.
- **NHREC Computer System and Network:** A computer system that is owned, purchased, and/or supported by NHREC, and includes all technology resources and access to

telecommunications networks (e.g. internet, local and wide area networks, hardware, software and communications services) division-wide and remotely.

- **Authorized User:** A NHREC Computer System and Network user whose access privileges have not been suspended or revoked.
- **NHREC Local Area Network:** The computer network using the private Internet Protocol (IP) address scheme (not directly accessible from the Internet) defined by NHREC Technology Department and accessed by wired or wireless connections.
- **Infringement:** When an individual inappropriately reproduces a work that is protected by a copyright.
- **Spamming:** An e-mail user sending annoying, non-school business, or unnecessary message(s) to an individual or a large number of people on a specific e-mail list or site.
- **Phishing:** The act of sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to persuade the user to surrender private information that will be used for identity theft.
- **Web based e-mail:** A web based system that performs the functions of a mail client allowing access to e-mail through the Internet.
- **Text messaging:** Text messaging is the common term for the sending of "short" (160 characters or fewer, including spaces) text messages from mobile phones using the Short Message Service(SMS).

NHREC will not be responsible for any information that may be lost, damaged or unavailable when using the NHREC Computer System and Network or for any information retrieved from the Internet.

NHREC is not responsible for any unauthorized charge or fee resulting from the use of the NHREC Computer System and Network.

In the event :filtering software, used to screen Internet sites for offensive material, is unsuccessful and authorized users gain access to inappropriate and /or harmful material, NHREC will not be liable.

Every effort will be made to avoid the violation of privacy of individuals or groups; however, NHREC Computer System and Network authorized users have no right of privacy and should have no expectation of privacy in materials sent, received, or stored in NHREC owned equipment within the Computer System.

15. OTHER POLICIES

New Horizons Regional Education Centers' Employee Handbook: Discrimination and Harassment

AUTHORITY REFERENCE

Code of Virginia, §22.1-70.2 *(Acceptable Internet use policies for public and private schools);* Children's Internet Protection Act *(Federal Communications Commission (Consumer & Governmental Affairs Bureau);* The Library of Virginia; Virginia Department of Education

Employee, Non- Employee, Student, and

Volunteer Technology Acceptable Use

Policy

Acceptance Form

I understand and will abide by the New Horizons Regional Education Centers Technology Acceptable Use Policy. I further understand that any violation of the regulations in New Horizons Regional Education Centers' Policy NH-3, Work Environment, Title: Technology Acceptable Use Policy is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, disciplinary and/or legal action may be taken.

Name (User)_____

(Please print)

Signature (User):_____

Date: _____