

NORTHWEST OHIO COMPUTER ASSOCIATION PROGRAM OF THE NORTHERN BUCKEYE EDUCATION COUNCIL NETWORK MANAGEMENT

SECURITY POLICY

The Board of Directors and staff of the Northwest Ohio Computer Association Program of the Northern Buckeye Education Council (hereafter referred to as **NWOCA**), recognizes the need for network security and management policies covering the integrated network services (voice, video, and data), provided to Ohio K-12 educational entities (hereafter referred to as **DISTRICT**). The Board adopts the following policy statements concerning access to, management of, and security of the network.

1. As a condition for obtaining networked services through **NWOCA**, **DISTRICT** agrees to obtain from **NWOCA** or its designee(s) at separate expense the additional transport service(s) and/or network equipment and devices necessary for transmission or receipt of information technology services at its locations. **DISTRICT** agrees that **NWOCA** maintains ownership and full administrative and management control of all managed network communications equipment attached to the network. Although the initial cost of such equipment is assessed to **DISTRICT** ownership of this equipment remains with **NWOCA** under all circumstances. Maintenance and/or replacement (at equivalent levels of technology), of this equipment is the responsibility of **NWOCA** or its designee(s). **DISTRICT** agrees that all equipment connected to the network must meet the approval of **NWOCA**. Devices attached not meeting **NWOCA**'s approval may be removed and/or disabled by **NWOCA** at **DISTRICT**'s (additional) expense.
2. **DISTRICT** assumes complete and full liability for all usage of network communications capabilities within its facilities, or within network subnets assigned to it.
3. **DISTRICT** acknowledges that unauthorized reproduction of copyrighted computer software or other electronic resources may be a violation of Federal copyright law and of Ohio criminal law, which also applies to other unauthorized use of computer facilities, network services, programs or data, and provides for punishment by substantial fines and/or imprisonment. The **NWOCA** Program supports these laws and encourages member educational entities, staff members, and students to fully comply with all such laws. Potential violations that come to the attention of the **NWOCA** staff will be investigated, and if substantiated, the educational entity will be required to fully comply with all applicable laws and **NWOCA** policies. If **DISTRICT** does not fully comply with all applicable laws and **NWOCA** policies, the matter will be referred to the General Assembly and/or Board of Directors of the **Northern Buckeye Education Council** for disciplinary action. Such action would occur at the direction of the Board of Directors or General Assembly of the **Northern Buckeye Education Council** and could result in the disqualification of **DISTRICT** from all programs of the **Northern Buckeye Education Council**.
4. **NWOCA** acknowledges that in the best interests of its owner-member school districts it may from time to time need to make exceptions and/or allowances to this policy. The Board grants the Executive Director the authority to grant temporary exceptions and/or allowances provided that the following occur:
 - a. The **DISTRICT** initiates a request in writing signed by the Superintendent.
 - b. The **DISTRICT** acknowledges that **NWOCA** can, and may, rescind any exception and/or allowance at any time.
 - c. The Executive Director deems the requested exception and/or allowance is in the best interests of both parties and will not subject other users of **NWOCA** to any undue liabilities and/or security risks.
5. Wireless local area network access points are encouraged to be placed under the ownership and full control of **NWOCA**. However, wireless local area network access points will be permitted to be owned and managed by the **DISTRICT** under the following conditions:
 - a. Wireless access points must be made physically secure from casual tampering, and the administrative password for the device must be changed from the vendor default.

- b. The SSID of all wireless access points must be changed from the vendor default. *Best practice would be to make the SSID have no obvious meaning that ties it to the organization, and it would be changed annually if administratively feasible. Best practice would also have the SSID broadcast disabled on all wireless access points.*
- c. Wireless access points must all have at least WEP (preferably WPA2) encryption enabled, if the volume of wireless devices permits, except in controlled areas where it is the intent to provide public access as permitted by **DISTRICT** policy and State and Federal regulations.
- d. WEP/WPA2 encryption keys must be created using a mixture of nonsense words and numbers using the highest encryption level possible on the wireless access points. *Best practice would be to change WEP/WPA2 encryption keys each school year if administratively feasible.*
- e. Wireless access points must be installed and/or configured in such a way that minimizes the coverage “footprint” beyond the facilities of **DISTRICT**.
- f. Wireless access points must use a form of static IP addressing, or one-to-one IP addressing, or Media Access Control (MAC) filtering must be enabled on all wireless access points, except in controlled areas where it is the intent to provide public access as permitted by **DISTRICT** policy and State and Federal regulations. *Best practice would be to enable MAC filtering and a form of static IP addressing or one-to-one IP addressing.*
- g. **DISTRICT** must lockdown visibility and changes to network control settings on all laptops authorized to use a wireless interface. *Best practice would be to enable a personal firewall on all laptops authorized to use a wireless interface (if so equipped by the operating system vendor).*
- h. **DISTRICT** must agree to educate district personnel that connecting unauthorized wireless access points to the **DISTRICT** network is not permitted without the consent of both the **DISTRICT** and **NWOCA**. Appropriate **DISTRICT** personnel must approve the connection of any wireless device to the network.
- i. **NWOCA** will maintain a listing of approved (supported) wireless network equipment at the following URL: <http://home.nwoca.org/Hardware/hardware.php?page=wireless>

6. **NWOCA** and the **Northern Buckeye Education Council** have herein designated the following items to be Security and/or Infrastructure records as defined in Ohio Revised Code §149.433: policy and procedure manuals and documents regarding Information Technology operations, security, disaster recovery, and business continuity processes; hardware, software, and network (detailed) architecture documents; disaster recovery planning documents; network security assessments; TCP/IP addressing assignments and associated metrics; application, network, and/or device logs containing IP addresses and/or user names; detailed telecommunications schematics; detailed network wiring schematics; detailed electrical wiring schematics; information technology and/or facility heating, ventilation, and air-conditioning detailed schematics; facility security system schematics and/or other information; and grants to the **NWOCA** Executive Director the authority to designate additional information items that, in his/her judgment would represent a potential risk to the security and integrity of **NWOCA**'s services and/or infrastructure should they become publicly available.

NETWORK PRIVACY AND ACCEPTABLE USE POLICY FOR STAFF MEMBERS

It is the intention of the _____ Board of Education to protect the privacy of staff members who use the school computers, computer network, and electronic messaging systems to the maximum extent possible given the operational and security needs of the District. The purpose of this policy is to identify the limitations on this privacy and the general restrictions applying to the use of computers and electronic messaging systems of the District.

Acceptable and Unacceptable Uses

The computers, computer network and messaging systems of the School District are intended for educational uses and work-related communications. Incidental use of the e-mail and voice mail systems by staff members for personal communications is permitted as long as such communications are limited in number, are initiated during non-work periods, and do not interfere with the primary intended uses of the system.

The following are uses which are unacceptable under any circumstances:

- the transmission of any language or images which are of a graphic sexual nature
- the transmission of jokes, pictures, or other materials which are obscene, lewd, vulgar, or disparaging of persons based on their race, color, sex, age, religion, national origin, or sexual orientation
- the transmission of messages or any other content which would be perceived by a reasonable person to be harassing or threatening
- the connection of any wireless device to the computer network unless specifically authorized by the district's network administrator
- uses that constitute defamation (libel or slander)
- uses that violate copyright laws
- uses that attempt to gain unauthorized access to another computer system or to impair the operation of another computer system (for example, the transmission of a computer virus or an excessively large e-mail attachment)
- any commercial or profit-making activities
- any fundraising activities, unless specifically authorized by an administrator

Security and Integrity

Staff members shall not take any action which would compromise the security of any computer, network or messaging system. This would include the unauthorized release or sharing of passwords and the intentional disabling of any security features of the system.

Staff members shall not take any actions which may adversely affect the integrity, functionality, or reliability of any computer (for example, the installation of hardware or software not authorized by the district's network administrator).

Staff members shall report to the district's network administrator and a School District administrator any actions by students or other staff members which would violate the security or integrity of any computer, network or messaging

system whenever such actions become known to them in the normal course of their work duties. **This shall not be construed as creating any liability for staff members for the computer-related misconduct of students or other staff members.**

Right of Access

Although the Board of Education respects the natural desire of all persons for privacy in their personal communications, and will attempt to preserve this privacy whenever possible, the operational and security needs of the District's computer network and messaging systems require that full access be available at all times. The School District therefore reserves the right to access and inspect any computer, device, or electronic media within its systems and any data, information, or messages which may be contained therein. All such data, information, and messages are the property of the School District and staff members should have no expectation that any messages sent or received on or through the School District's systems will always remain private.

Legal Ref.: ORC 3313.20, 3313.47 *Children's Internet Protection Act of 2000*, 47 USC § 254 (h), (l)

RECEIPT FORM

I acknowledge receipt of the "Network Privacy and Acceptable Use Policy for Staff Members" of the _____ School District (revised ___ / ___ / 200__).

_____ Staff Member Signature PLEASE

PRINT: _____ Date above

signed: _____

***** OFFICE USE ONLY *****

Login Name: _____

Password: _____

ACCEPTABLE USE AND INTERNET SAFETY POLICY FOR THE COMPUTER NETWORK OF THE

_____ SCHOOL DISTRICT

The _____ School District is pleased to make available to students access to interconnected computer systems within the District and to the Internet, the world-wide network that provides various means of accessing significant educational materials and opportunities.

In order for the School District to be able to continue to make its computer network and Internet access available, all students must take responsibility for appropriate and lawful use of this access. Students must understand that one student's misuse of the network and Internet access may jeopardize the ability of all students to enjoy such access. While the School's teachers and other Staff will make reasonable efforts to supervise student use of network and Internet access, they must have student cooperation in exercising and promoting responsible use of this access.

Below is the Acceptable Use and Internet Safety Policy ("Policy") of the School District and the Data Acquisition Site that provides Internet access to the School District. Upon reviewing, signing, and returning this Policy as the students have been directed, each student will be given the opportunity to enjoy Internet access at School and is agreeing to follow the Policy. If a student is under 18 years of age, he or she must have his or her parents or guardians read and sign the Policy. The School District cannot provide access to any student who, if 18 or older, fails to sign and submit the Policy to the School as directed or, if under 18, does not return the Policy as directed with the signatures of the student and his/her parents or guardians.

Listed below are the provisions of your agreement regarding computer network and Internet use.

If you have any questions about these provisions, you should contact the person that your School has designated as the one to whom you can direct your questions. If any user violates this Policy, the student's access will be denied, if not already provided, or withdrawn and he or she may be subject to additional disciplinary action.

I. PERSONAL RESPONSIBILITY

By signing this Policy, you are agreeing not only to follow the rules in this Policy, but are agreeing to report any misuse of the network to the person designated by the School for such reporting. Misuse means any violations of this Policy or any other use that is not included in the Policy, but has the effect of harming another or his or her property.

II. TERM OF THE PERMITTED USE

A student who submits to the School, as directed, a properly signed Policy and follows the Policy to which she or he has agreed will have computer network and Internet access during the course of the school year only. Students will be asked to sign a new Policy each year during which they are students in the School District before they are given an access account.

III. ACCEPTABLE USES

A. **Educational Purposes Only.** The School District is providing access to its computer networks and the Internet for *only* educational purposes. If you have any doubt about whether a contemplated activity is educational, you may consult with the person(s) designated by the School to help you decide if a use is appropriate.

B. **Unacceptable Uses of Network.** Among the uses that are considered unacceptable and which constitute a violation of this Policy are the following:

1. uses that violate the law or encourage others to violate the law. Don't transmit offensive or harassing messages; offer for sale or use any substance the possession or use of which is prohibited by the School District's Student Discipline Policy; view, transmit or download pornographic materials or materials that encourage others to violate the law; intrude into the networks or computers of others; and download or transmit confidential, trade secret information, or copyrighted materials. Even if materials on the networks are not marked with the copyright symbol, you should assume that all materials are protected unless there is explicit permission on the materials to use them.
2. uses that cause harm to others or damage to their property. For example, don't engage in defamation (harming another's reputation by lies); employ another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; upload a worm, virus, "trojan horse," "time bomb" or other harmful form of programming or vandalism; participate in "hacking" activities or any form of unauthorized access to other computers, networks, or information systems.
3. uses that jeopardize the security of student access and of the computer network or other networks on the Internet. For example, don't disclose or share your password with others; don't impersonate another user; don't connect wireless devices to the computer network or attempt to intercept wireless communications.
4. uses that are commercial transactions. Students and other users may not sell or buy anything over the Internet. You should not give others private information about you or others, including credit card numbers and social security numbers.

C. **Netiquette.** All users must abide by rules of network etiquette, which include the following:

1. Be polite. Use appropriate language. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language.
2. Avoid language and uses which may be offensive to other users. Don't use access to make, distribute, or redistribute jokes, stories, or other material which is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
3. Don't assume that a sender of e-mail is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her e-mail address to third parties. This should only be done with permission or when you know that the individual would have no objection.
4. Be considerate when sending attachments with e-mail (where this is permitted). Be sure that the file is not too large to be accommodated by the recipient's system and is in a format which the recipient can open.

IV. INTERNET SAFETY

A. **General Warning; Individual Responsibility of Parents and Users.** All users and their parents/guardians are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his or her use of the computer network and Internet and stay away from these sites. Parents of minors are the best guide to materials to shun. If a student finds that

other users are visiting offensive or harmful sites, he or she should report such use to the person designated by the School.

- B. **Personal Safety.** Be safe. In using the computer network and Internet, do not reveal personal information such as your home address or telephone number. Do not use your real last name or any other information which might allow a person to locate you without first obtaining the permission of a supervising teacher. Do not arrange a face-to-face meeting with someone you “meet” on the computer network or Internet without your parent’s permission (if you are under 18). Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet in a secluded place or in a private setting.
- C. **“Hacking” and Other Illegal Activities.** It is a violation of this Policy to use the School’s computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.
- D. **Confidentiality of Student Information.** Personally identifiable information concerning students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian or, if the student is 18 or over, the permission of the student himself/herself. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers. A supervising teacher or administrator may authorize the release of directory information, as defined by Ohio law, for internal administrative purposes or approved educational projects and activities.
- E. **Active Restriction Measures.** The School, either by itself or in combination with the Data Acquisition Site providing Internet access, will utilize filtering software or other technologies to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors. The School will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material which is inappropriate for minors.

Internet filtering software or other technology-based protection systems may be disabled by a supervising teacher or school administrator, as necessary, for purposes of bona fide research or other educational projects being conducted by students age 17 and older.

The term “harmful to minors” is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file, or other visual depiction that -taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

- depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals;
- taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

V. PRIVACY

Network and Internet access is provided as a tool for your education. The School District reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the School District and no user shall have any expectation of privacy regarding such materials.

VI. FAILURE TO FOLLOW POLICY

The user's use of the computer network and Internet is a privilege, not a right. A user who violates this Policy, shall at a minimum, have his or her access to the computer network and Internet terminated, which the School District may refuse to reinstate for the remainder of the student's enrollment in the School

District. A user violates this Policy by his or her own action or by failing to report any violations by other users that come to the attention of the user. Further, a user violates this Policy if he or she permits another to use his or her account or password to access the computer network and Internet, including any user whose access has been denied or terminated. The School District may also take other disciplinary action in such circumstances.

VII. WARRANTIES/INDEMNIFICATION

The School District makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this Policy. It shall not be responsible for any claims, losses, damages or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet under this Policy. By signing this Policy, users are taking full responsibility for his or her use, and the user who is 18 or older or, in the case of a user under 18, the parent(s) or guardian(s) are agreeing to indemnify and hold the School, the School District, the Data Acquisition Site that provides the computer and Internet access opportunity to the School District and all of their administrators, teachers, and staff harmless from any and all loss, costs, claims or damages resulting from the user's access to its computer network and the Internet, including but not limited to any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardian(s) agree to cooperate with the School in the event of the School's initiating an investigation of a user's use of his or her access to its computer network and the Internet, whether that use is on a School computer or on another computer outside the School District's network.

VIII. UPDATES

Users, and if appropriate, the user's parents/guardians, may be asked from time to time to provide new or additional registration and account information or to sign a new Policy, for example, to reflect developments in the law or technology. Such information must be provided by the user (or his/her parents or guardian) or such new Policy must be signed if the user wishes to continue to receive service. If after you have provided your account information, some or all of the information changes, you must notify the person designated by the School to receive such information.

STUDENT'S AGREEMENT

Every student, regardless of age, must read and sign below:

I have read, understand and agree to abide by the terms of the foregoing Acceptable Use and Internet Safety Policy. Should I commit any violation or in any way misuse my access to the School District's computer network and the Internet, I understand and agree that my access privilege may be revoked and School disciplinary action may be taken against me.

Student name (PRINT CLEARLY) Home phone

Student signature Date

Address User (place an "X" in the correct blank): I am 18 or older _____ I am under 18 _____

If I am signing this Policy when I am under 18, I understand that when I turn 18, this Policy will continue to be in full force and effect and agree to abide by this Policy.

PARENT'S OR GUARDIAN'S AGREEMENT

Student's name

To be read and signed by parents or guardians of students who are under 18:

As the parent or legal guardian of the above student, I have read, understand and agree that my child or ward shall comply with the terms of the School District's Acceptable Use and Internet Safety Policy for the student's access to the School District's computer network and the Internet. I understand that access is being provided to the students for educational purposes only. However, I also understand that it is impossible for the School to restrict access to all offensive and controversial materials and understand my child's or ward's responsibility for abiding by the Policy.

I am therefore signing this Policy and agree to indemnify and hold harmless the School, the School District and the Data Acquisition Site that provides the opportunity to the School District for computer network and Internet access against all claims, damages, losses and costs, of whatever kind, that may result from my child's or ward's use of his or her access to such networks or his or her violation of the foregoing Policy. Further, I accept full responsibility for supervision of my child's or ward's use of his or her access account if an when such access is not in the School setting.

I hereby give permission for my child or ward to use the building-approved account to access the School District's computer network and the Internet.

Parent or Guardian name(s) (PRINT CLEARLY) Home phone

Parent or Guardian signature(s) Date

Address

ADOPTED:

REVISED:

Legal References: Children's Internet Protection Act of 2000 (H.R. 4577, P.L. 106-554)

Communications Act of 1934, as amended (47 U.S.C. 254[h],[l]) Elementary and Secondary Education Act of 1965, as amended (20 U.S.C. 6801 et seq., Part F)