

COMPUTER NETWORK FOR EDUCATION

The Board of Education recognizes that as telecommunications and other new technologies increase the number of ways that information may be accessed, communicated and transferred by members of society, those changes also alter teaching and learning. The Board considers access to a computer network, including the internet, to be a powerful and valuable educational tool. The Board is committed to the use of computer-related technology as a tool to advance and promote teaching and learning.

The computer network significantly alters the information landscape for schools by opening classrooms to a broader array of resources, including the internet, online databases, bulletin boards, e-mail and various software applications. The network will open classrooms to electronic information resources which may not have been screened by educators for use by students of various ages. The Board generally supports access by students to diverse information-rich resources concomitant with the development of appropriate skills to analyze and evaluate such resources by staff members.

Electronic information research skills are now necessary for the proper preparation of citizens and future employees during an Age of Information. The Board expects that staff will blend thoughtful use of such information throughout the curriculum and that the staff will provide guidance and instruction to students in the appropriate use of such resources.

The Board authorizes student use of personal devices to access the District's computer network if the student complies with the District's registration process, as well as the provisions of this policy and regulation, unless his/her parent opts out such student from computer use and/or network access. Failure to register or abide by this policy and regulation will result in revocation of access and possibly disciplinary action in accordance with the Code of Conduct.

All users of the District's computer network and the internet must understand that access is a privilege, not a right, and that access entails responsibility. All users are required to demonstrate appropriate conduct on school computers and networks, just as they are required to adhere to the District's code of conduct when on school grounds or while involved in any school-related functions. Failure to comply with this Policy and Regulation may result in disciplinary action as well as suspension and/or revocation of computer access privileges. The code of conduct applies to all aspects of network use and communications. The network is provided for students and staff to conduct research and to communicate with others.

The Internet Use & Safety Policy is available for review by parents or guardians on request, and parents or guardians should be familiar with it. The Internet Use & Safety Policy contains restrictions on accessing inappropriate and/or harmful material on the Internet through the District's computer network in order to protect users. In addition, the District will employ filtering technology and will monitor and attempt to properly channel on-line activities of students. However, there is a wide range of material available on the Internet that may not be in keeping with the particular views of the families or the students. The District recognizes that parents have primary responsibility for transmitting their particular set of values to their children and that the parents or guardians of minors are ultimately responsible for setting and conveying standards that their children should follow when using the Internet, media and information sources. Parents are

also responsible for monitoring the students' use of the Internet and the District's network if students are using the District's computer network to access the Internet from home.

The District believes that the benefits to students of Internet access that result from the vast amount of information resources and opportunities for collaboration outweigh the disadvantages of such access. However, parents or guardians may believe otherwise and therefore, may specifically request that the District not allow their child to have Internet access on the District's computer network. Such request must be made in writing, signed and dated by the parent(s) or guardian and delivered to the student's building principal. Parents or guardians must make separate written requests for each child that will be denied Internet access by the District.

In such cases where Internet use is part of the curriculum of a course or program, students will be permitted to complete alternative projects approved by the student's teacher, except if the student is enrolled in an elective course which requires demonstrated proficiency using these resources.

The Board authorizes the Superintendent of Schools to establish regulations governing the use and security of the District's computer network. All users of the District's computer network and equipment shall comply with this policy and accompanying regulations.

The Superintendent shall designate staff to oversee the use of District computer resources. Responsibilities shall include maintenance, security and integrity of networks and equipment, the delivery of in-service programs for the training and development of District staff in computer skills, and for the integration of computer use into classroom instruction. The Superintendent, working in conjunction with appropriate District staff, will be responsible for the purchase and distribution of computer software and hardware throughout District schools. District staff shall prepare a comprehensive multi-year technology plan that shall be revised periodically to reflect changing technology and/or District needs.

With increased concern about identity theft, unwarranted invasion of privacy and the need to protect personally identifiable information, prior to students being directed by staff to use any cloud-based educational software/application, staff must get approval from the Director of Technology. The Director of Technology will determine if a formal contract is required or if the terms of service are sufficient to address privacy and security requirements, and if parental permission is needed.

Adoption date: February 4, 2009
Revised: January 20, 2010
Revised: January 20, 2016

COMPUTER NETWORK FOR EDUCATION REGULATION

The following rules and regulations govern the use of the District's computer network system and access to the Internet and e-mail accounts.

I. Administration

- The Superintendent of Schools shall prepare appropriate procedures for implementing this policy and for reviewing and evaluating its effect on instruction and student achievement.
- The Superintendent shall designate staff to oversee the District's computer network. These staff may include a Director of Technology to manage the infrastructure and hardware resources, and a Coordinator of Instructional Technology to manage instructional software, curriculum design and professional development.
- Together, these staff shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.
- These staff shall be responsible for disseminating and interpreting District policy and regulations governing use of the District's network at the building level with all network users.
- The District shall provide employee training for proper use of the network and will ensure that staff supervising students using the District's network provide similar training to their students, including providing copies of District policy and regulations governing use of the District's network.
- District computer staff shall make every effort to maintain the integrity of the network, including critical software updates and virus protection.
- All parent requests for students to "opt out" of Internet access on the District's computer network shall be kept on file in the main office of each school.

II. Program Development

In order to integrate the use of electronic resources within the framework of the approved District curriculum, District personnel will review and evaluate resources in order to offer materials that comply with Board guidelines governing the selection of instructional materials. In this manner, staff will provide developmentally appropriate guidance to students as they make use of telecommunications and electronic information resources within the approved instructional program. All students will be informed by staff of their rights and responsibilities as users of the District network prior to gaining access to that network, either as an individual user or as a member of a class or group.

As much as possible, access to District information resources will be designed in ways that point students to those that have been reviewed, evaluated and approved prior to use. While students may be able to move beyond those resources to others that have not been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Students may pursue electronic research independent of staff supervision, unless his/her parent opts out such student from computer use and/or network access.

The District believes that the benefits to students from access to important information resources and opportunities for growth through collaboration exceed the potential problems and disadvantages. The District, recognizes, however, that parents and guardians of minors are responsible

for setting and conveying the standards that their children should follow when using media and information sources. To that end, the Lindenhurst Public Schools support and respect each family's right to decide whether or not to opt out of independent student access. No student's grade shall be diminished if a parent or guardian opts out of independent access to the Internet or electronic resources, except if the student is enrolled in an elective course which requires demonstrated proficiency using these resources.

III. Internet Access

- Access to Internet resources comes with the understanding that some material accessed is inaccurate. Additionally, some material may be contrary to community standards and inappropriate for classroom use. All staff and students, therefore, must be aware of the need to critically evaluate information and resources gathered from the Internet.
- Independent student use of Internet and electronic information resources will be permitted unless a student's parent opts out such student from computer use and/or network access.
- Students will be provided with access to Internet resources during class time as determined by the teacher, and before, during and after the school day as facilities are available unless a student's parent opts out such student from computer use and/or network access.
- All students (except those who have been opted out) and staff will have individual network accounts. These accounts grant access to the World Wide Web.
- Students are not to participate in chat rooms.
- Students will not have e-mail accounts provided by the District. The possibility exists that students may access their private e-mail accounts via the Internet access provided by the District.
- A staff member will be required to monitor any and all student network activities.
- The District will provide staff members with web-based e-mail accounts.
- In order to access the Internet students must use the District's network.

IV. Staff E-mail Guidelines

The District believes that one of the foundations of quality education is excellent communication. This is reflected in regular communication among various members of our educational community; i.e., among teaching colleagues, between teachers and students, between administrators and teachers and between parents and teachers. In order to enhance the communication, the District provides e-mail accounts for staff. These accounts will allow staff members to communicate in more efficient ways:

- E-mail communication is available at a time and place that is convenient to the user.
- E-mails tend to be more succinct than oral communications.
- Responses can be planned in advance.
- Collaborative efforts can be enhanced.

The following guidelines have been established to assist the members of our educational community in using e-mail communication successfully:

- Members of the professional staff, including administrators, teachers and support staff, are expected to check their e-mail regularly.

- Professional staff members are expected to respond to all messages received in a timely fashion. However, the method of response can be of their choice; e.g. an e-mail message may be responded to via the telephone.
- In any instance where a parental signature is required by law or District policy, the policy remains as is: e-mail will not be an acceptable substitution for field trip permission forms, absence notes, etc.
- Building level administrators will inform parents that emergency information should not be left on teachers' e-mail accounts, but rather, should be communicated directly to the main office.
- Staff members who receive questionable messages should immediately inform their appropriate administrator, save the message(s) and print them. Staff adhering to this reporting procedure will not be held accountable for the receipt of such messages.
- Mass mailing of letters or e-mails by teaching staff require prior approval from the appropriate administrator.
- Whenever an administrator posts a group mailing to staff, a hard copy of that message will be posted in a central, previously defined area.

To best utilize our resources, each mailbox has been allocated *limited* space on the mail server. *To maximize on that* space, it is recommended that users abide by the following suggestions:

- Delete messages after reading them if there is no need to refer back to them.
- Delete messages over 30 days old.
- Save attachments as needed to a local directory and delete the message from the mail server.

V. Acceptable Use and Conduct

- Access to the District's computer network is provided solely for educational purposes and research consistent with the District's mission and goals.
- Use of the District's computer network is a privilege, not a right. Inappropriate use may result in the suspension or revocation of that privilege.
- Communications on the network are often public in nature. All users are expected to abide by the generally accepted rules of network etiquette. This includes being polite and using only appropriate language. Abusive language, vulgarities and swear words are all inappropriate.
- Each individual in whose name an access account is issued is responsible at all times for its proper use. Each user will be issued a login name and password and must protect the individual account and personal password from disclosure.
- Network users identifying a security problem on the District's network must notify the appropriate teacher, administrator or computer network coordinator. Under no circumstance should the user demonstrate the problem to anyone other than to the District official or employee being notified.

Any network user identified as a security risk or having a history of violating the District's computer use guidelines may be denied access to the District's network.

- Users must not leave a workstation computer unattended while logged on to a network account – this leaves files vulnerable and/or will allow others to commit acts which will be traced to the user who was logged in at the time.
- In order to protect electronic data, staff members are expected to backup data completely and frequently, as this is the most important line of defense against loss of data. While the District will backup data stored on the file server, users are urged to backup critical files on their own disk media.

VI. Prohibited Activity and Use

The following is a list of prohibited activity concerning use of the District's computer network. Violation of any of these prohibitions may result in discipline or other appropriate penalty, including suspension or revocation of a user's access to the network.

- Using the network for commercial activity, including advertising or purchasing or selling anything online (unless authorized for District purposes).
- Infringing on any copyrights or other intellectual property rights, including copying, installing, receiving, transmitting or making available any copyrighted software on the District computer network.
- Using the network to access social networking sites.
- Using the network to play online games. Using the network to receive, transmit or make available to others obscene, offensive, or sexually explicit material.
- Using the network to receive, transmit or make available to others messages that are racist, sexist, abusive or harassing to others.
- Using another user's account or password.
- Attempting to read, delete, copy or modify the electronic mail (e-mail) of other system users and deliberately interfering with the ability of other system users to send and/or receive e-mail.
- Forging or attempting to forge e-mail messages.
- Engaging in vandalism. Vandalism is defined as any malicious attempt to harm or destroy District equipment or materials, data of another user of the District's network or of any of the entities or other networks that are connected to the Internet. This includes, but is not limited to, creating and/or placing a computer virus on the network.
- Using the network to send anonymous messages or files.
- Using the network to receive, transmit or make available to others a message that is inconsistent with the District's Code of Conduct.
- Revealing the personal address, telephone number or other personal information of oneself or another person.
- Using the network for sending and/or receiving personal messages.
- Sharing confidential information about students. This includes, but is not limited to, grades, Individual Education Plans, attendance and disciplinary records.
- Intentionally disrupting network traffic or crashing the network and connected systems.
- Installing personal software or using personal disks on the District's computers and/or network without the permission of the appropriate District official or employee.
- Using District computing resources for commercial or financial gain or fraud.
- Stealing data, equipment or intellectual property.
- Gaining or seeking to gain unauthorized access to any files, resources, or computer or phone systems, or vandalize the data of another user.

- Wastefully using finite District resources.
- Changing or exceeding resource quotas as set by the District without the permission of the appropriate District official or employee.
- Using the network while access privileges are suspended or revoked.
- Using the network in a fashion inconsistent with directions from teachers and other staff and generally accepted network etiquette.
- Any use of network resources that disrupts the overall goals of the District.

VII. No Privacy Guarantee

Network storage areas are public spaces and belong to the District. Network administrators may review files and communications to maintain system integrity and ensure that users are using the system responsibly. All messages sent over Lindenhurst's computer and communication systems are the property of the District. Since the system is to be used for educational and business purposes, users should have no expectation of privacy associated with the information stored in or sent through these systems. If a student is using his/her personal device to access the District's network, the student must keep school work separate from personal files, since school work is subject to District access.

All messages sent by e-mail are Lindenhurst Public Schools' records. Messages sent over the District's internal e-mail systems are not subject to the privacy provisions of the Electronic Communications Privacy Act of 1986 and, therefore, may be read by the District's management and system administrators. The District reserves the right to access and view any material stored on District equipment or any material used in conjunction with the District's computer network.

VIII. Sanctions

All users of the District's computer network and equipment are required to comply with the District's policy and regulations governing the District's computer network. Failure to comply with the policy or regulation may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

In addition, illegal activities are strictly prohibited. Any information pertaining to or implicating illegal activity will be reported to the proper authorities. Transmission of any material in violation of any federal, state and/or local law or regulation is prohibited. This includes, but is not limited to materials protected by copyright, threatening or obscene material or material protected by trade secret. Users must respect all intellectual and property rights and laws.

IX. District Responsibilities

Information security on a network is a function of both equipment and the people who use it. The District will establish many safeguards in the networked equipment, such as passwords, virus protection and firewalls. The District expects that staff will do its part to help protect information on all the systems that they use. The District will provide and maintain reasonable access in classrooms and department offices to equipment designed to provide access to the network, the Internet and e-mail

accounts. The District will provide opportunities for professional development on the use of the network and electronic resources.

The District makes no warranties of any kind, either expressed or implied, for the access being provided. Further, the District assumes no responsibility for the quality, availability, accuracy, nature or reliability of the service and/or information provided. Users of the District's computer network and the Internet use information at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided.

The District will not be responsible for any damages suffered by any user, including, but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by its own negligence or the errors or omissions of any user. The District also will not be responsible for unauthorized financial obligations resulting from the use of or access to the District's computer network or the Internet.

Further, even though the District may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of the District policy and regulation.

Adoption date: February 4, 2009
Revised: January 20, 2010
Revised: January 20, 2016

LINDENHURST PUBLIC SCHOOLS
Student User Agreement

As a user of the Lindenhurst Public Schools computer network, I understand that when I am using the Internet or any other telecommunication technology, I must adhere to all rules of courtesy, etiquette and laws regarding access and copying of information as prescribed by either Federal, State, or local laws, and the Lindenhurst Union Free School District's policies and regulations. My signature below means that I have read the "Computer Network for Education" policy and regulation (lindenhurstschools.org/Assets/policies_documents/AUP2011.PDF), discussed it with my parent/guardian, and I hereby agree to comply with the terms and conditions and all of the rules contained in such policy and regulation, to communicate over the network in a responsible fashion, and to honor all relevant laws and restrictions.

 Student Signature

 Date

 Parent Signature

 Date

 Name of Student

 School

 Grade

 Student ID Number
 (District Issued)

 Birth Date

 Street Address

 Home Telephone Number

Computer Network for Education Policy is online at:

www.lindenhurstschools.org/Assets/policies_documents/AUP2011.PDF

Approved: January 20, 2010

Revised: January 20, 2016

Disclaimer: Although the District has taken reasonable precautions, we can neither guarantee nor be responsible for the security, accuracy or appropriateness of content distributed through our network. The District will not be liable for any financial or legal obligations arising from the unauthorized use of our system.

LINDENHURST PUBLIC SCHOOLS

Computer Network for EducationStaff User Agreement

I have read, understand and will abide by the terms and conditions contained in the Lindenhurst Union Free School District's *Computer Network for Education* Policy No. 4526 and corresponding Regulation 4526-R. I understand and acknowledge that I have no right to privacy or reasonable expectation of privacy when I use a District computer, the District's Computer Network and/or the Internet, and that the District reserves the right to monitor such usage as it deems appropriate in order to protect the District and ensure compliance with District policies and regulations. I acknowledge that the District may monitor and search any District computer I use, as well as my use of the District's Computer Network and my computer communications, including but not limited to my use of email and the Internet. I further understand that any violation of this policy and/or regulation is strictly prohibited, may be unethical and constitute a criminal offense and result in my access to privileges being revoked and/or the District taking disciplinary action and/or appropriate legal action against me. Further, in consideration for the privilege of using the District's computers and Computer Network and in consideration for having access to the Internet, I hereby agree to release, defend, hold harmless, and indemnify the Lindenhurst Union Free School District, its Board of Education, Board members, and employees, against any and all claims, damages, judgments, and attorneys' fees of any nature arising out of my use, or inability to use, District computers and/or the District's Computer Network and/or the Internet.

 Name of Staff Member

 Signature

 Date

 Building Assigned

 Position

Computer Network for Education Policy is online at:

www.lindenhurstschools.org/Assets/policies_documents/AUP2011.PDF

Approved: January 20, 2010

Revised: March 21, 2012

Revised: January 20, 2016