LOVE SERVICE
Cleary School for the Deaf
301 Smithtown Boulevard, Nesconset, New York 11767-2077 631-588-0530 (V & TTY)
www.clearyschool.org

COMPUTER NETWORK AND INTERNET ACCESS ACCEPTABLE USE

Cleary School for the Deaf is committed to the optimization of student learning and teaching. Cleary School considers a computer network, including the internet, to be a powerful and valuable educational and research tool, and encourages the use of computers and computer-related technology in our School classrooms for the purpose of advancing and promoting learning and teaching.

Within financial limitations, computers, computer networks and the internet will be made available to students, faculty and staff. The technology resources at the School (e.g., all networking, hardware and software, the Internet, e-mail, telephone equipment, digital still and video, voice mail, fax machines and supporting telephone lines, and all communication equipment) are provided to support the educational and administrative activities of the School and should be used for those purposes. An individual's use of the School's computer resources must be in support of education and research and consistent with the educational objectives of Cleary School.

The computer network can provide a forum for learning various software applications and, through online databases, bulletin boards and electronic mail, can significantly enhance educational experiences and provide statewide, national and global communications opportunities for staff and students.

When an individual accesses computers, computer systems and/or computer networks, including the internet provided by the School, the individual assumes certain responsibilities and obligations. Access to the School's computers, computer systems and/or computer networks is subject to federal, state and local law, as well as the School's policy. The use of the School's computers, computer networks and the internet is a privilege, not a right, and inappropriate use will result in the cancellation of privileges and/or disciplinary action by the School principal.

All users of the School's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility. The School reserves the right to control access to the Internet for all users of its computers and network. The School may either allow or prohibit certain kinds of online activity, or access to specific websites.

The Executive Director designates a computer coordinator (Director of Business Operations) to oversee the use of the School's computer resources. The coordinator will oversee that all staff and students read, acknowledge and sign off on an annual Acceptable Use agreement.

For all School employees, the contents of electronic communications, including email, instant messaging, listservs, blogs, wikis, social networking sites (Facebook, LinkedIn, Twitter, Instagram, etc.), should be composed with professionalism. Because many of these tools occupy online public spaces, the potential to bring harm to oneself, to others, and to the School must be recognized, as recipients may forward messages to locations where there is no control over future dissemination.

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 Business Operations.

Authorized Use

Authorized users of the School's computer resources include members of the governing administrators, supervisors, faculty, staff, students, parent/guardian and any other person who has been granted access to the School's computer resources. Unauthorized use is strictly prohibited. By utilizing the School's computer resources or personally-owned equipment, the user consents to the School's exercise of its authority and rights as set forth in this Policy with respect to the School's computer resources, as well as with respect to any information or communication stored or transmitted over the School's computer resources.

Faculty, staff members, and students (where applicable) may be provided with e-mail accounts and Internet access. Whenever a user ceases being a member of the School community or if such user is assigned a new position and/or responsibilities, use of the School's computer resources for which he or she is not authorized in his or her new position or circumstances shall cease and property returned. When a School employee separates from service from the School, access to all School accounts and email is disabled. All School business being conducted electronically must be performed with a School account or service. Employees should not use private email accounts. Email used for School purposes may be subject to FOIL. There is no expectation of privacy when utilizing School email.

Privacy Expectations

The School's computer resources, including all telephone and data lines, are the property of the School. The School reserves the right to access, view or monitor any information or communication stored on or transmitted over the network, or on or over equipment that has been used to access the Schools network and it may be required by law to allow third parties to do so. Electronic data, e.g., may become evidence in legal proceedings. In addition, others may inadvertently view messages or data as a result of routine systems maintenance and monitoring or misdelivery.

The School's monitoring of its Systems will include, but not be limited to, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing communications, logins and other uses of the Systems, as well as keystroke capturing and/or other network sniffing technologies. The reasons for which the School will obtain such access include, but are not limited to: maintaining the Systems; preventing or investigating allegations of abuse or misuse of the Systems; ensuring compliance with software copyright laws; monitoring and ensuring that school operations continue appropriately during an employee's absence or unavailability. Accordingly, employees must provide the School with any access codes or passwords applicable to these Systems.

Likewise, because the School will be monitoring these Systems, employees should have no expectation of privacy as it relates to any data or communications created with, transmitted by or stored on the School's Systems, including those marked as "personal" or confidential".

Any and all telephone conversations or transmissions, electronic mail or transmissions, or internet access or usage by an employee by any electronic device or system, including but not limited to the use of a computer, telephone, wire, radio or electromagnetic, photoelectronic or photo-optical systems may be subject to monitoring at any and all times and by any lawful means.

Permissible Use

1. All users must not act in ways that invade the privacy of others or fail to comply with all legal restrictions regarding the use of electronic data. All users must also recognize and not violate the intellectual property

rights of others.

2. All users must maintain the confidentiality of student information in compliance with federal and state law including, but not limited to, FERPA, HIPAA and Education Law, section 2-d.
3. Disclosing (including but not limited to via e-mail, voice mail, Internet instant messaging, social media, chat rooms or on other types of Web pages) confidential or proprietary information related to the School is prohibited.
4. All users must refrain from acts that waste School computer resources or prevent others from using them. Users will not access, modify or delete others' files or system settings without express permission. Tampering of any kind is strictly forbidden. Deliberate attempts to tamper with, circumvent filtering or access, or degrade the performance of the School's computer resources or to deprive authorized users of access to or use of such resources are prohibited.
5. Students may not send broadcast email or broadcast voicemail.
6. Users are responsible for both the content and possible effects of their messages on the network. Prohibited activity includes, but is not limited to, creating or propagating viruses, material in any form (text, sound, pictures or video) that reflects adversely on the School, "chain letters" (which proffer incentives to relay them to others), inappropriate messages (including discriminatory, bullying or harassing material), and billable services.
7. Official email communications must be professional and meet the standards of other School publications bearing in mind that the writer is acting as a representative of the School and in furtherance of the School's mission.
8. Users are prohibited from using personal links and addresses such as blogs, YouTube videos, etc. in School email unless used in the furtherance of business of the School as part of the curriculum of the School.
9. The School recognizes the value of teacher and professional staff inquiry, investigation and communication using new technology tools to enhance student learning experiences. The School also realizes its obligations to teach responsible and safe use of these new technologies. Social media, including social networking sites, have great potential to connect people around the globe and enhance communication. Therefore, the Executive Director and administrators encourage the use of social media tools and the exploration of new and emerging technologies to supplement the range of educational services.

   For purposes of this Policy, the definition of public social media networks or Social Networking Sites (SNS) are defined to include: websites, Web logs (blogs), wikis, social networks, online forums, virtual worlds, video sites and any other social media generally available to the School community which do not fall within the School's electronic technology network (e.g., Facebook, MySpace, Twitter, LinkedIn, Flickr, Vine, Instagram, SnapChat, blog sites, etc.). Employees are required to maintain the highest levels of professionalism when communicating in their professional capacity as educators. Employees have a responsibility to address inappropriate behavior or activity on these networks, including compliance with all applicable School Policies and Regulations.

10. The signature portion of the user's email may not include external links or graphics that are unrelated to the content of the email.
11. Altering electronic communications to hide the identity of the sender or impersonate another person is illegal, considered forgery and is prohibited.
12. Users will abide by all copyright, trademarks, patent and other laws governing intellectual property. No software may be installed, copied or used on School equipment except as permitted by law and approved by the Director of Business Operations or his/her designee in accordance with the procedures established for use of software/hardware with the School's computer resources. All software license provisions must be strictly adhered to.
13. Students are not permitted to record classroom instruction without the express permission of the teacher.

14. The School fully supports the experimental educational and business use of digital resources including, but not limited to, software, third party applications, websites, web-based programs and/or any applications/resources which require a login/password. Since the installation of digital resources, other than School-owned and School tested digital resources could damage the School's computer resources, compromise student data/privacy and/or interfere with others' use, digital resources downloaded from the Internet or obtained elsewhere must be approved by the Director of Business Operation or his/her designee. Digital resources may not be installed onto any School owned or School-leased computer unless in compliance with the School's policies concerning purchasing and computer resources. Once digital resources have been approved by the Director of Business Operations, installation will be scheduled and performed.

Inappropriate Materials

1. The School prohibits faculty, staff and students from developing, maintaining, and transmitting pornography in any form at school, including, but not limited to, magazines, posters, videos, electronic files or other electronic materials.
2. Accessing the School's network or equipment to create, access, download, edit, view, store, send or print materials that are illegal, harassing, discriminatory, sexually explicit or graphic, pornographic, obscene, or which constitute sexting or cyberbullying or are otherwise inconsistent with the values and general standards for community behavior of the School is prohibited. The School will respond to complaints of harassing or discriminatory use of the School's computer resources in accordance with School policies. These provisions are not intended to prohibit an authorized user from carrying out his or her assigned educational, employment or administrative function.

Use of Personal Electronic Devices/School Issued Devices

The School authorizes use of personal electronic device(s) and/or school issued devices to access the internet using the School's computer resources for educational purposes. Individuals connecting to the internet using the School's computer resources are required to comply with the School's Internet Safety Policy, as well as the provisions of this policy and regulation. Failure to abide by this policy and regulation will result in disciplinary action including, but not limited to, revocation of access to the School's computer resources.

"Personal electronic devices" or "School issued devices" include, but are not limited to, personal laptops, smart phones, portable storage media, all recording devices, all Internet connected devices and handheld devices such as laptops, iPods and iPads and include student owned and school issued devices. With classroom teacher approval, students may use their own devices to access the Internet for educational purposes. The School reserves the right to monitor, inspect, and/or confiscate personal electronic devices when administration has reasonable suspicion that a violation of school policy has occurred.

The School maintains a "public" wireless network, a "private" wireless network, an "instructional" wireless network and a "hard wired" network. The "hard wired" and "private" wireless networks are limited only to school-owned and managed devices. Any attempt to connect a personal electronic device to either of these networks will be considered a violation of this policy. The "public" wireless network is the sole network that students and faculty may connect to using their personal electronic devices. The School reserves the right to alter or disable access to the "public" wireless network as it deems necessary without prior notification.

Personal electronic devices that have the ability to offer wireless access to other devices must not be used to provide that functionality to others in any School building. The ability to connect personal electronic devices to the School's wireless network is a privilege and not a right. When personal electronic devices are used in a School building or on the School's wireless network, the School reserves the right to:

1. make determinations on whether specific uses of the personal electronic device is consistent with this policy
2. log internet use and monitor storage disk space utilized by such users
3. remove or restrict the user's access to the internet and suspend the right to use the personal electronic device in the School's facilities at any time if it is determined that the user is engaged in unauthorized activity or in violation of School policy

In addition, when staff members choose to use their own personal electronic devices to perform job related functions, the following will apply:

1. The School may choose to maintain a list of approved mobile devices and related software applications and utilities. The School reserves the right to deny any staff member permission to utilize a personal electronic device within the boundaries of the School. The Executive Director or his/her designee reserves the right to make these decisions in his/her discretion.
2. Personal electronic devices connected to the internet using the School's computer resources and/or wireless network must have updated and secure operating systems and proper forms of anti-virus and anti-malware protection. Staff must not make any attempt to connect devices that are not properly secured.
3. The cost to acquire all personal electronic devices is the responsibility of the staff member. Services that include a financial cost to the School, such as phone options or other "apps" are not allowed. The School does not agree to pay such charges and staff who desire these options must assume all costs incurred for such charges.
4. Personal electronic devices are not covered by the Schools insurance if lost, stolen or damaged. Loss or damage to any personal electronic device is solely the responsibility of the staff member. If lost or stolen, the loss should be reported immediately to the Director of Business Operations or his/her designee so that appropriate action can be taken to minimize any possible risk to the School's computer system and the School overall.
5. Staff members shall remain responsible for the maintenance of personal electronic devices, including maintenance to conform to School standards. Staff members also assume all responsibility for problem resolution, as well as the use and maintenance of functional, up-to-date anti-virus and anti-malware software and any other protections deemed necessary by the Director of Business Operations or his/her designee.
6. Staff must also meet any expectations of continuity in formatting of files, etc. when making changes to documents for work purposes (i.e., do not change the format of a file so that the original file is unusable on School-owned hardware/software).
7. All personal electronic devices used with the School's computer resources are subject to review by the Director of Business Operation or his/her designee, or individuals/entities designated by the Executive Director, if there is reason to suspect that the personal electronic device is causing a problem to the School's computer resources.
8. The use of personal electronic devices in the course of a staff member's professional responsibilities may result in the equipment and/or certain data maintained on it being subject to review, production and/or disclosure (i.e., in response to a FOIL request, discovery demand or subpoena). Staff members are required to submit any such information or equipment, when requested.
9. Staff members using a mobile device, personal or School-owned, are responsible for compliance with all security protocols normally used in the management of School data on conventional storage infrastructure are also applied on that mobile device. All School defined processes for storing, accessing and backing up data must be used on any device used to access the School's computer system.

Further, the School will not be liable for the loss, damage, theft, or misuse of any personal electronic device(s)

brought to school. The School will bear no responsibility nor provide technical support, troubleshooting, or repair of electronic devices owned by anyone other than the. Students and staff are responsible for understanding and inquiring about the use of technology prior to engaging in such use.

The person to whom the School has issued an electronic device will be liable for the loss, damage, theft, or misuse of said electronic device(s) issued by the School. In addition, a student or staff member may be responsible for the full replacement cost of the device if the loaned device is lost, damaged, stolen or misused.

Confidentiality and Privacy Rights

Individuals must take all reasonable precautions to prevent unauthorized access to accounts or data by others, both inside and outside the School. Individuals will not leave any devices unattended with confidential information visible. All devices are required to be locked down when an individual steps away from the device, and settings enabled to freeze and lock after a set period of inactivity.

Data files and electronic storage areas shall remain School property, subject to the School's control and inspection. The Director of Business Operations or his/her designee may access all such files and communications without prior notice to ensure system integrity and that users are complying with requirements of this policy.

Security

1. Each user is responsible for the security and integrity of information stored on his or her computer or voice mail system. Computer accounts, passwords, security codes and other types of authorization are assigned to individual users and must not be shared with or used by others. The School, at its sole discretion, reserves the right to bypass such passwords and to access, view or monitor its systems and all of their contents. By accessing the School's system, the individual consents to the School's right to do so.
2. Removing School computer resources from the School's facilities and/or relocating School computer resources (not including portable technology devices) requires prior authorization from the Director of Business Operations or his/her designee.
3. Unless approved by the Director of Business Operations, modem use is prohibited on computers that are directly connected to the School network. Personal network appliances may not be connected to the School network and may be confiscated.
4. Storage of copyrighted materials such as music, video and games is prohibited.
5. Users may not attempt to circumvent or subvert the security provisions of any other system. Without authorization from the Director of Business Operations or his/her designee, no one may attach a server to or provide server services on the School's network.

The Internet at the School's Campus

1. There are risks involved with using the Internet. To protect personal safety, Internet users should not give out personal information to others on websites, chat rooms or other systems. The School cannot guarantee that users will not encounter text, pictures or references that are objectionable. Responsible attitudes and appropriate behavior are essential in using this resource. As with e-mail, information that a user places on the Internet is akin to sending a postcard rather than a sealed letter. Its contents may be accessed by system administrators in this School and elsewhere.
2. Users must be aware that some material circulating on the Internet is copyrighted and subject to all copyright laws. Materials taken from the Internet must be properly cited.
3. Users must be aware that some material circulating on the Internet is illegally distributed. Users must

never use the School's system to download illegally distributed material.

4. Users are cautioned not to open email attachments or download any files from unknown sources in order to avoid damaging School computers and bringing destructive viruses into the School's system. Anything questionable should be reported immediately to the Director of Business Operations or his/her designee.
5. With permission, students, faculty and staff may create or modify web pages on the School's web servers. To ensure the integrity of these sites, users must abide by the School's web practices. It is the user's responsibility to update and maintain all links and content, keeping in mind the Inappropriate Materials section and the copyright requirements.

School Limitation of Liability

The School does not warrant in any manner, express or implied, that the functions or the services provided by or through the School system will be error-free or without defect. The School shall not bear any liability for any damage suffered by users including, but not limited to, loss of data or interruption of service. Similarly, the School shall not bear any liability for financial obligations that arise out of the unauthorized or illegal use of the system.

Users of the School's computer resources at all campuses, including internet use, do so at their own risk. Each user is responsible for verifying the integrity and authenticity of the information that is used and provided. Further, even though the School may use technical or manual means to regulate access and information, these methods do not provide a foolproof means of enforcing the provisions of all School policies and regulations.

Policy Enforcement and Sanctions

1. All members of the School community are expected to assist in the enforcement of this policy. Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, the loss of computer, telephone or network access privileges, disciplinary action, monetary damages and/or dismissal/termination from the School. Some violations may constitute criminal offenses as defined by local, state and federal laws, and the School may initiate or assist in the prosecution of any such violations to the full extent of the law.
2. Any suspected violation of this policy should be reported immediately to the Director of Business Operations, as well as to the Principal (if the suspected violator is a student), or the Executive Director (if the suspected violator is a faculty or staff member).

Additional Policies and Guidelines for Use of School Computer Resources

Use of the School's computer resources in the School and its campuses, must comply with the following:

1. Cyberbullying, and sexting using sexually explicit, graphic, threatening or obscene language or images, or otherwise using language or images inconsistent with the values and general standards for community behavior of the School are prohibited.
2. Anyone leaving such inappropriate messages on voice mail may face disciplinary action.
3. Anyone receiving a threatening message should record/save the message and report the incident to the Principal. The Director of Business Operations will attempt to trace the message and report the results to the Principal and the Executive Director.
4. Use of voice mailboxes for commercial purposes or advertising is not permitted.
5. Use of security codes is required in order to guarantee privacy for mailbox users.

Wireless Policy and Guidelines

Cellular phones and walkie-talkies are provided to selected members of the School by the Business Office.

Wireless devices including, but not limited to, laptops, iPhones, iPod Touches, iPads and notebook computers are provided to staff members and/or students of the School by the Director of Business Operations. The Business Office maintains the inventory for all these devices, auditing of wireless use by the staff, and efficient and effective resolution of billing and service-related issues. The use of wireless technology has been identified by the School as useful in maintaining communications among the School community and School personnel in emergency situations or situations where immediate access to an employee is necessary. The use of such wireless technology is subject to the requirements of the School's technology and telecommunications practices. By using wireless devices provided by the School, the individual consents to the School's exercise of its authority and rights as set out in this policy.

Cellular Phone Usage

Purpose

All School-issued cellular phones shall be used for the purpose of supporting the Schools education and business objectives. This policy is intended to facilitate effective School operations relating to cellular phone usage, encourage the responsible use of School-provided cellular phones, provide guidelines for appropriate cellular phone use, and help manage cellular phone usage costs.

Authorized Users

A list of those employees to whom cellular phones will be given for school business purposes shall be maintained by the Director of Business Operations and reviewed annually by the Executive Director. This list shall also state with specificity, for each employee, the basis for the issuance of a School cellular phone.

Acceptable Use Guidelines

1. Cellular phones shall be used only for necessary phone calls in furtherance of school business purposes. Charges or fees for personal cellular phone calls shall be reimbursed by the employee to the School.
2. The School shall monitor whether employee cellular phone use or expenses are unreasonable, excessive, personal, unauthorized, or unwarranted.
3. School cellular phones shall not be used for the purpose of illegal transactions, harassment, or other violations of School policies or law.
4. Cellular phone service contract rights and equipment shall be the property of the School, and any applicable determinations or changes as to them shall be made by the Business Office.
5. Employees shall have no expectation of privacy in the use of School cellular phones. All cellular phone bills for School-issued phones are the property of the School and will be used as appropriate to investigate the personal use of School-issued cellular phones.
6. School cellular phones are valuable and should be handled with due care. If loss, theft, or damage to a School cellular phone results from the known negligence of the employee to whom such phone is assigned, the employee will be required to reimburse the School for the repair or purchase of replacement equipment.
7. Upon request, School-issued cellular phones shall be returned to the appropriate Business Office.
8. The School may discontinue cellular phone privileges at any time.

The Executive Director or his/her designee shall conduct regular cost-benefit analyses to determine whether the current cellular phone usage is advantageous to the School, as well as whether cellular phone service plans should be changed in order to reduce costs and maximize the benefit to the School.

Policy on Wireless Device/Radio Use

The School insists that all employees act responsibly in their jobs so as not to endanger the lives of themselves

or others. No telephone communication, business or personal, is so necessary or urgent that it cannot be postponed or interrupted until such time as the involved person can participate in the phone call without compromising safety. Safe driving is always the first responsibility. The School actively discourages the use of hand-held cellular phones, and other wireless communication devices, while driving cars, trucks and golf carts both on and off campus, during School work time or on School business.

Further, employees should not dial, text, email or otherwise violate the law related to the use of electronic devices while driving on School business. If an employee must engage in any of the above activities, he or she must pull over to a safe location off the roadway and out of traffic, stop and park the vehicle before doing so. Stopping in a roadway breakdown lane is by its very nature dangerous and therefore is not considered a safe location by the School.

The School acknowledges that members of the school administration, members of the facilities department and computer services and athletic trainers often use two way radios and radio telephones in the School in the performance of their daily duties. In addition, the use of wireless devices by administration are both prevalent and necessary. These employees are reminded to use these devices in such a manner so as not to compromise safety.

The failure to comply with this policy may result in the loss of privileges/access to the School's computer resources and possible disciplinary action consistent with law or the applicable collective bargaining agreement.

The Executive Director, working in conjunction with the Business Office for the School, the computer network coordinator and the instructional materials planning committee, will be responsible for the purchase and distribution of computer software and hardware throughout the schools. They shall prepare a comprehensive multi-year technology plan which shall be revised as necessary to reflect changing technology and/or School's needs.

Failure to comply with Cleary School for the Deaf's policy and regulations for use of the network may result in disciplinary action as well as suspension and/or revocation of computer access privileges.