

North Shore Central School District

Chromebook Policies, Procedures, and Other Information

The focus of the 1:1 program within the North Shore Schools is to provide tools and resources to the 21st Century Learner. Increasing access to technology is essential for that future, and one of the learning tools to accomplish this goal for our students will be through the use of 1:1 mobile devices. The individual use of iPads and Chromebooks is a way to empower students to maximize their full potential and to prepare them for college and the workplace.

Learning results from the continuous dynamic interaction among students, educators, parents and the extended community. Technology transforms the teacher from a director of learning to a facilitator of learning. Effective teaching and learning with iPads and Chromebooks integrates technology into the curriculum, providing students with valuable learning opportunities that otherwise would not be accessible.

The policies, procedures and information within this document apply to all iPad and Chromebook use within the North Shore Schools, as well as any other device considered by the Administration to come under this policy. Teachers may set additional requirements for use in their classroom.

IMPORTANT: The following pages of this document must be signed and returned only to CENTRAL OFFICE before a student may receive a Chromebook:

Page 33: Chromebook Protection Plan

Page 34: Chromebook MOU

Page 35: Student AUP Agreement

Page 36: Parent AUP Agreement

Please visit <https://www.northshoreschools.org/chrome> to find the most current versions of all Chromebook-related forms, paperwork, and policies.

1. RECEIVING/RETURNING YOUR CHROMEBOOK

Upon successful completion of paperwork and protection plan payment, all students are eligible to receive the following equipment:

Acer Chromebook (\$299)

Acer Power Adapter (\$20)

Belkin Protective Sleeve (\$10)

Once issued, the individual student **Chromebook and all related accessories including sleeve and power adapter (hereafter collectively referred to as “Chromebook”)** will remain in the possession of each student throughout his or her entire enrollment at North Shore. Students will always retain their Chromebooks during all school breaks and at the end of each school year unless otherwise specified. Students are expected to return every September from summer break with his or her Chromebook.

Students that are in 12th grade or the Life Skills program and are graduating from the District must turn in their Chromebooks prior to leaving North Shore. Cap and gowns will only be issued to a graduating student upon receipt of his or her Chromebook. **Chromebook Protection Plans do not cover lost or missing Chromebooks in this circumstance.**

Students who graduate early, withdraw, are expelled, or terminate enrollment within the North Shore Schools for any other reason must return his or her individual school Chromebook to the Technology Office on or before the date of departure from the District. Failure to do so will result in a withholding of final student grades or academic transcripts until the Chromebook is returned or the District is reimbursed for the full cost of the Chromebook (\$299) and all related accessories (\$20). **Chromebook Protection Plans do not apply towards this type of loss.**

Similarly, if a departing student returns a Chromebook that was not covered by a protection plan in damaged or non-working condition, he or she will be responsible for reimbursing the full cost of replacing that Chromebook. Failure to return the Chromebook or provide the District with reimbursement in either case will also result in a theft report being filed with the local Police Department. The student may additionally be subject to criminal prosecution or civil liability.

2. CHROMEBOOK AND RELATED ACCESSORY CARE

Students are responsible at all times for the general care of their District Chromebook. **Students must take the necessary precautions at all times when his or her Chromebook is not in use on by storing it in a secure location.** Chromebooks that are damaged or fail to work properly must be taken to the Technology Office or the building's computer lab for an evaluation of the equipment.

2.1 General Precautions

- The Chromebook is school property and all students will follow the District's Technology Acceptable Use Policy (hereafter referred to as "AUP") for Chromebooks and technology within the North Shore Schools (http://www.northshoreschools.org/boe/Policies/4000_series.pdf#page=78).
- Students are responsible for keeping their Chromebook battery sufficiently charged for school each day.
- The power adapter must be inserted carefully into the Chromebook to prevent damage.
- Chromebooks must remain free of any writing, drawing, stickers, or labels that are not placed on the Chromebook by the North Shore Technology Department.
- Labels that have been placed on the Chromebook by the Technology Department must not be removed.
- **The Chromebook must be stored in its protective sleeve when not in use.**
- Students should never run or roughhouse in any way with a Chromebook in his or her possession.
- **Chromebooks must never be left in an unlocked locker, visible in a car, or any other unsupervised area.**
- If a student brings his or her Chromebook to a Physical Education period or after-school athletics event, he or she is responsible for storing the Chromebook in a secure, locked location.

Violation of any of the above precautions may result in the nullification of any protection plan that covers the Chromebook.

2.3 Screen Care

The Chromebook screen can be damaged if subjected to rough treatment. The screen is particularly sensitive to damage from excessive pressure placed on top of it. Students must observe the following precautions:

- Do not lean any part of your body on the top of the Chromebook when it is closed.
- Do not place anything near or on top of the Chromebook that could put pressure on the screen.
- Do not closet the lid of the Chromebook when there is any object in-between the screen and keyboard.
- Do not place the Chromebook in-between any books or other class materials.
- Only use a clean, non-abrasive cloth to clean the screen, and no cleansers of any type.
- Do not “bump” the Chromebook against lockers, walls, car doors, floors, etc.
- Do not drop the Chromebook on tables, chairs, couches, beds, cushions, etc., even from a short height.

3. USING YOUR CHROMEBOOK AT SCHOOL

Chromebooks are intended for use at school each day. In addition to teacher expectations for Chromebook use, school messages, announcements, calendars and schedules may be accessed using the Chromebook. Students must be responsible to bring their Chromebook to all classes, unless specifically instructed not to do so by their teacher.

3.1 Chromebooks Left At Home

If students leave their Chromebook at home, they are responsible for completing the coursework as if they had their Chromebook present. The technology department will not be responsible for providing any student with a loaner Chromebook for devices that are left home under any circumstances.

3.2 Chromebook Hardware Defects

If a Chromebook becomes unusable due to a hardware defect that is **NOT** caused by accidental damage, misuse, or mishandling of the Chromebook, a replacement unit will usually be issued to a student within the same day **provided that the student drops off the Chromebook to his or her building's computer lab at or before 9 AM**. Any Chromebook undergoing repairs as a result of accidental damage, misuse, or mishandling of the Chromebook will be replaced under the terms and conditions set forth in the District's Chromebook replacement policies.

3.3 Charging Your Chromebook's Battery

Chromebooks must be brought to school each day in a fully charged state. Students need to charge their Chromebooks each evening by plugging them into an electrical wall outlet only with the supplied genuine Chromebook power adapter. The technology department will not be responsible for providing any student with a loaner Chromebook or power adapter for devices that are not charged under any circumstances.

3.4 Home Internet Access

Students are permitted to configure additional wireless networks on their Chromebooks for use at home. However, students are not permitted to configure or use non-District wireless networks while in District. Any attempt to do so will be treated as a violation of the District's AUP and will result in the confiscation of the Chromebook and further disciplinary actions.

4. MANAGING YOUR FILES & SAVING YOUR WORK

All students are issued a District Chromebook with a District Google account. In virtually all circumstance, all data that the students will create will automatically be stored in Google's Drive cloud storage.

4.1 File Management / Backing Up

There are several methods that the District recommends for managing data on the Chromebook:

- Email: Students and teachers can exchange copies of course-related files through their District email accounts.
- GSuite: Students can use Gsuite's sharing abilities to provide access to work that they have saved in Drive to other students and teachers in real-time collaboration.
- Cloud-Based Services: Students also have the option to utilize any number of free cloud-based options such as OneDrive or Dropbox. The District will allow the use of such services by students on their Chromebooks, but the District cannot be held responsible for the support of these services or the data that the students may store on these services.

4.2 Network and Student Email Connectivity

The North Shore School District makes no guarantee that the wireless network will be accessible 100% of the time or fully responsive in all building locations as it relates to latency and speed, nor can it guarantee the uninterrupted availability of student email services. In the event that either provided service is inaccessible or performing poorly/unpredictably, the District will not be responsible for lost or missing data.

5. APPS/EBOOKS/OTHER MEDIA ON CHROMEBOOKS

5.1 General Guidelines

- Music, videos, images, and non-educational apps loaded onto the Chromebook may not be opened, accessed, displayed, or played back at any time in class unless otherwise specified by the teacher for instructional purposes.
- Presence of guns, weapons, pornographic materials, vulgar language, alcohol, drug, gang related symbols or other inappropriate elements found on a student's Chromebook will be treated as a violation of the District's AUP and result in the confiscation of the student's Chromebook and further disciplinary actions.
- All sound on the Chromebook must be muted at all times in class unless otherwise specified by the teacher for instructional purposes.

5.2 District-Provided Content

The District will provide at its own expense commercial extensions, ebooks, web-based services, and other media that it deems to be educationally relevant to students. The District may offer additional content for use in a particular course at the request of a classroom teacher or curriculum director.

5.3 Chrome Webstore

The Chrome Web Store (<https://chrome.google.com/webstore>) is available for student use. The District employs a combination of an internet filter and an extension blacklist that prevents students from accessing content that is deemed inappropriate or instructionally disruptive.

5.4 Circumvention of Managed Settings

All student Chromebooks are initially provisioned by the Technology Department for the purposes of managing District Chromebooks in a secure and organized fashion. Any attempts by students to circumvent any District management settings through software alterations, operating system restoration, "power washing", or other methods of hacking will be treated as a violation of the District's AUP and result in the confiscation of the student's Chromebook and further disciplinary actions.

All Chromebooks are enrolled in several administrative services in order to provide limited filtering, tracking, and remote management capabilities for the technology department.

Deliberately circumventing or removing the Chromebook from any of these management

services may additionally result in the nullification of any protection plan that covers the Chromebook.

5.5 Inspection/Recall

Students may be selected at random to provide their Chromebook for inspection or recall by the Technology Department at any time. Summer recalls may also occur for one or more entire grades if acceptable use changes require that all Chromebooks are updated to remain in compliance.

5.6 Software Updates

The Technology Department will be responsible for remotely deploying all Chromebook operating system updates. Students will only need to restart their Chromebooks in order to receive the updates.

6. ACCEPTABLE USE

The use of North Shore School District's technology resources is a privilege, not a right. The privilege of using any technology resources provided by the District is not transferable or extendible by students to people or groups outside the District and terminates when a student is no longer enrolled in the District. This policy is provided to make all users aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If a person violates any of the User Terms and Conditions named in this policy, as well as the District AUP, privileges may be terminated, access to the school District technology resources may be denied, and the appropriate disciplinary action shall be applied. The North Shore School District's Student Code of Conduct shall be applied to all student infractions. Violations may result in disciplinary action up to and including suspension/ expulsion for students. When applicable, law enforcement agencies may be involved.

6.1 Parent/Guardian Responsibilities

Talk to your children about values and the standards they should follow on the use of the Internet just as you do on the use of all media information sources such as television, telephones, movies, and radio. Establish a policy of digital responsibility at home with your child's use of his or her Chromebook. If necessary, parents may also optionally enforce appropriate Internet use at home with a personal web filter.

Parents or guardians are also expected to be familiar with the contents of this handbook, select his or her preferred Chromebook protection plan option, and complete and submit all necessary paperwork and payments to Central Office in a timely fashion to avoid delays in issuing your child's Chromebook.

6.2 District Responsibilities

- Provide Internet and student email service to students with District Chromebooks.
- Provide students free access to required commercial content.
- Provide in-District Internet filtering of inappropriate materials as required by CIPA.
- Provide technical support to aid students in Chromebook troubleshooting and replacements.

6.3 Students Responsibilities

- Use his or her Chromebook in a responsible and ethical manner.
- Obey general school rules concerning behavior and communication that applies to Chromebook use.

- Use his or her Chromebook in an appropriate manner so as to not damage it.
- Secure his or her Chromebook when not in use to protect against loss or theft.
- Keeping his or her Chromebook in the District-issued protective sleeve when not in use.
- Keeping his or her Chromebook fully charged and ready for use each day.
- If a student receives email or other communications containing inappropriate or abusive language, or if the subject matter is questionable, the student must report the incident to his or her building principal.
- Report any damage, loss, or theft of his or her Chromebook to the Technology Department as soon as it is discovered.
- Turn in to the Technology Department any unattended Chromebooks that are discovered on school grounds.
- Students who graduate early, withdraw, are expelled, or terminate enrollment for any other reason must return their individual school Chromebook on or before the date of enrollment termination.

6.4 Student Activities Strictly Prohibited

- Illegal transmission of copyrighted materials.
- Any action that violates existing Board policy or public law.
- Sending, accessing, uploading, downloading, or distributing offensive, profane, threatening, pornographic, obscene, or sexually explicit materials.
- Use of plagiarism sites or services offering term papers, book reports, exam answers, or any other forms of student work.
- Messaging services, social media, games, or any other Internet service in class without the express permission of the classroom teacher.
- Use of social media or messaging services to bully, harass, or intimidate others.
- Use of peripherals for external data access without prior approval from the Technology Department.
- Installation of operating systems or other software on his or her Chromebook that are not from the District.
- Changing of Chromebook settings so as to cause damage or inaccessibility to the device from District staff.
- Use of apps or other content in class that is in violation of the District's AUP or creates a disruption to the instructional environment.
- Use of the Chromebook as a concealed recording device of another party that has not given explicit consent to be recorded.
- Gaining unauthorized access to any other user's accounts, email, or other data.

- Exchanging Chromebooks with other students, and/or switching Chromebook identification labels to conceal damage.
- Use of the school's Internet/email accounts for financial or commercial gain or any illegal activity.
- Use of anonymizing and/or masquerading communication proxy services.
- Students are not permitted to release personal information for any reason over the District's network.
- Participation in fraud, forgery, identity theft, or other forms of illegal behavior.
- Any malicious attempts to vandalize or destroy District hardware, software, or data.
- Transmission or accessing materials that are obscene, offensive, threatening, or otherwise intended to harass, intimidate, or demean recipients.
- Bypassing the North Shore Internet filter through the use of a VPN or web proxy.

6.5 Chromebook Care

- Students will be held responsible for maintaining their individual Chromebooks and keeping them in good working order and available for class as required by teachers.
- Chromebooks must be charged and ready for school each day.
- Only labels or stickers approved by the North Shore Technology Department may be applied to the Chromebook.
- All Chromebook accessories furnished by the school District must be used with only normal wear and no alterations.
- Chromebooks that experience a hardware malfunction or are damaged by accidental student misuse or mishandling must be reported immediately to the Technology Department.
- Students will be responsible for the full cost of replacing a Chromebook (\$299) that is damaged intentionally through vandalism or gross negligence, and any protection plan's provisions will be rendered void.
- Chromebooks that are lost stolen must be reported immediately to the Technology Department. The student must attempt to locate the Chromebook within 24 hours of the reported incident, after which he or she must file a police report if the Chromebook remains missing. The report must be sent to Central Office for processing before a replacement Chromebook process can begin.

7. PROTECTING & STORING YOUR CHROMEBOOK

7.1 Chromebook Identification

Student Chromebooks are uniquely assigned to a student in the following ways:

- Chromebook labeled with student's name
- Record of Chromebook serial number
- Completion of District's AUP by parent and student
- Enrollment of Chromebook in District's device management services

7.2 Storing Your Chromebook

When students are not using their Chromebooks in school, they should be stored in their lockers. Nothing should be placed on top of the Chromebook when stored in the locker. Students are encouraged to take their Chromebooks home every day after school, regardless of whether or not they are needed. Chromebooks should not be stored in a student's vehicle at school or at home, and should never be left unattended or in the possession of another person.

7.3 Chromebooks Left in Unsupervised Areas

Under no circumstances should Chromebooks be left in unsupervised areas. Unsupervised areas include the school grounds and campus, the lunchroom, computer labs, locker rooms, library, unlocked classrooms, dressing rooms, and hallways. Chromebooks that are reported as lost or stolen as a result of being left unattended in an unsupervised area may result in the nullification of any protection plan that covers the Chromebook.

If a Chromebook is lost or found in an unsupervised area, **it must be returned to the building's computer lab or District's Technology Office.** The recovered Chromebook will only be released to the student that it is assigned to.

8. REPLACING A CHROMEBOOK

8.1 Cost of Replacements

Should the damaged Chromebook NOT be covered by a District protection plan, the student will be responsible for the replacement value of a Chromebook (\$299). This includes but is not limited to:

- Missing keys from keyboard
- Inoperability from hacking
- Dented/cracked/scratched screen or body
- Damaged ports (USB/HDMI/Charging/Headphones)
- Inoperable power button
- Damaged protective sleeve
- Broken/bent/frayed power adapter
- Lost or stolen items

Damaged or lost accessories such as protective sleeves (\$10) and power adapters (\$20) will always be invoiced for the actual replacement cost or require replacement by the student, as none of these items are covered by the District protection plan.

Under no circumstances should a parent attempt to repair a damaged District Chromebook with a third-party service. This will result in the nullification of a protection plan or retainer agreement, and parents will assume the full cost of replacement (\$299).

8.2 District Protection Plans

NOTE: The most current versions of Chromebook replacement paperwork are always available on the District's website: <https://www.northshoreschools.org/chrome>

District Chromebook Protection Plans are available for students and parents to cover the full replacement cost of a District Chromebook (**excluding accessories such as power adapters and protective sleeves**) in the event of theft, loss, or accidental damage.

Protection plans are available for purchase from the beginning of the school year to June 1st. After this date, students will have to wait until the start of the new school year before reporting a damaged or missing Chromebook. Please note that availability of Technology Department staff will vary during extended holidays and breaks, which may result in unexpected delays to processing new protection plan requests.

The details of District Protection Plans are as follows:

- **The protection cost is \$50.00* (non-refundable)** to cover the full cost of one Chromebook replacement (\$299) incident. **Protection plans do not cover the loss of any Chromebook accessories (power adapters or protective sleeves)**, and the student or parent assumes full responsibility for replacement or reimbursement of these items in all circumstances. Any attempt to repair the Chromebook with a third-party service will result in the nullification of the protection plan, and parents will assume the full cost of replacement.
- Once purchased, a protection plan will be linked to a specific Chromebook and “follow it” indefinitely across all school years. The protection plan coverage will also extend into the summer break and other vacation periods throughout the school year. Once that specific Chromebook with the linked protection plan is damaged or reported as missing/stolen, that protection plan is then considered “consumed” by the Chromebook loss. A new protection plan must be purchased prior to receiving a replacement Chromebook. This new protection plan will subsequently link to the new Chromebook and follow it in the same way.
- **Students who graduate, withdraw, are expelled, or terminate enrollment within the North Shore Schools for any other reason must return his or her individual school Chromebook to the Technology Office on or before the date of departure from the District. Protection Plans cannot be applied towards this type of loss.**
- **A limit of two District protection plans**** may be purchased for any one student in perpetuity of his or her North Shore enrollment from 5th grade to graduation. This counter does not reset between school years, and the record of Chromebook damage or loss follows the student through the end of his or her enrollment at North Shore.
- If a student consumes two Chromebook replacement/protection plan cycles and requests a **third Chromebook, a retainer agreement** must be initiated between the parent/guardian and the District. The retainer agreement acts the same way as the protection plan by linking to the replacement Chromebook and following it indefinitely across all school years. The retainer agreement coverage will also extend into the summer break and other vacation periods throughout the school year.

- A security deposit via a check or money order for \$299 made payable to North Shore Schools will be required as a condition of establishing the retainer agreement before the replacement Chromebook can be issued to the student.
- If the student under a retainer agreement returns his or her Chromebook to the Technology Department at or before the end of his or her North Shore enrollment without damage to the device, the full deposit of \$299 will be returned to the parent.
- If a student under a retainer agreement reports his or her Chromebook as lost or stolen, or does not return it at the end of his or her North Shore enrollment, or returns it with visible or operational damage, the full \$299 deposit will be forfeit to the District and not reimbursed under any circumstances. If any related accessories are not returned, applicable fees will be deducted from the deposit for each missing accessory item.
- If a Chromebook is deemed intentionally lost or damaged as a result of pre-meditated student negligence or misuse, any District protection plan or retainer agreement covering that Chromebook will be rendered void and the student will incur the full cost of replacement.
- **A police report must be filed by a parent or guardian in response to a missing or stolen Chromebook within 24 hours of the incident occurring.** This process is discussed in detail in the next section. A copy of the report must be sent to Central Office for processing before a replacement Chromebook process can begin.

**** The FIRST \$50 Protection Plan fee will be waived for students whose families qualify for and are registered with the District for Free and Reduced Lunch***

***** Students whose families qualify for and are registered with the District for Free and Reduced Lunch are not subject to this protection plan limit. If at any time a student's free and reduced lunch registration is denied or revoked, the protection plan limit will be reinstated.***

IMPORTANT: All Chromebook replacement forms, payments, or police reports must be reported only to Lois Straber in Central Office. All other District teachers and staff will be explicitly instructed to not accept any forms or payments from students, and the District cannot be held responsible for any monetary loss that results in a student not following these procedures.

District Protection Plans and all associated paperwork or payments must be submitted to Central Office prior to receiving a District Chromebook:

North Shore CSD
Attn: Lois Straber
112 Franklin Avenue
Sea Cliff, NY 11579

Any additional questions not covered in this section may be referred to Lois Straber at 516.277.7815 or straberl@northshoreschools.org.

9. CHROMEBOOK REPLACEMENT POLICY

IMPORTANT: Chromebook replacements will be handled from the beginning of the school year to June 1st. After this date, students will have to wait until the start of the new school year before reporting a damaged or missing Chromebook.

Please allow 24-48 hours lead time for each step in this process, as timeframes may vary depending upon staff availability.

9.1 Chromebook Damage

If a student damages his or her Chromebook (cracked screen, broken ports, etc.), it must be delivered for evaluation **by that student** with the District-issued protective case to the following locations by building:

- High School: Computer Lab (Mr. Torre/Mr. LaFranca)
- Middle School: Library Office (Mr. Spampinato)
- Glen Head: Computer Lab (Ms. Statile)
- Glenwood Landing: Computer Lab (Ms. Barry)
- Sea Cliff: Computer Lab (Ms. Tanner)

Do not deliver damaged Chromebooks to classroom teachers, guidance counselors or building secretaries under any circumstances, as this will cause delays in the process or potential loss of the Chromebook.

9.2 Chromebook Loss

If a student **loses** his or her Chromebook, the following steps must be taken **within 24 hours of the loss**:

- The student or parent must report the loss to the designated person in his or her building (detailed above), and agree to spend a period of **24 hours backtracking** to locations visited with the Chromebook during the previous day's activities.
- If the Chromebook is still missing after this search, the parent must file a police report with the **3rd Police Precinct (214 Hillside Ave, Williston Park, 11596)** that documents the loss. The number for the operator is **516.573.6300**.
- A copy of the completed police report must be submitted to Central Office for review.

9.3 Central Office Notification

If a damaged Chromebook is found to require replacement or a Chromebook is still reported as

lost after 24 hours of search, the Technology Office will notify Central Office of the incident:

- Central Office will mail paperwork to the parent's home address for completion.
- If you do not receive mailed paperwork within this timeframe, the most current Chromebook forms and policies can also be downloaded at <https://northshoreschools.org/chrome>
- If this is a **first replacement Chromebook**, the paperwork will require parents to submit a non-refundable payment of **\$50 protection payment** to cover the new Chromebook.
- If this is a **second replacement Chromebook**, Central Office will contact the parents to discuss payment and liability options for a new Chromebook.

9.4 Paperwork/Payment

Paperwork received by parents must be completed and submitted in full with payment to the following address by regular mail or in-person delivery:

North Shore CSD
Attn: Lois Straber
112 Franklin Avenue
Sea Cliff, NY 11579

- Payments must be made payable to **North Shore CSD**, and may be personal check or money order only.
- **Do not submit paperwork or payment to classroom teachers, guidance counselors, or building secretaries under any circumstances, as this will cause delays in the process or potential loss of the paperwork and payment.**
- Upon receipt of the paperwork and payments, Central Office will review and ensure that all submissions are verified as accurate and complete.
- Central Office will send a receipt of successful submission of paperwork and payment via postal mail.
- If either paperwork or payment is incomplete or missing, Central Office will notify the parent of the required corrections.

9.5 New Chromebook Pickup

Once paperwork and payment are verified, Central Office will notify the Technology Office that the student is cleared to receive a replacement Chromebook:

- A replacement Chromebook will be provisioned for the student.
- If the student attends the High School, his or her new Chromebook will be available for pick-up from **each building's computer lab**.
- If the student attends the Middle School, his or her new Chromebook will be **delivered**

to the student by the building's computer lab aide.

9.6 Accessories

The District will issue only one power adapter per issued Chromebook. All costs to replace lost Chromebook power are the responsibility of the student.

District Technology Acceptable Use Policy

4526-E.2

NORTH SHORE SCHOOL DISTRICT

COMPUTER NETWORK

ACCEPTABLE USE POLICY

Please read the following before signing the attached legally binding contract.

Introduction

Internet access is now available to students, teachers, staff, administrators, and community members in the North Shore School District. The District's goal in providing such access is to promote educational excellence in the North Shore Schools by facilitating resource sharing innovation, and communication. The District regards this access as a privilege, not a right.

The North Shore School District's Wide Area Network Computer Network is an electronic network with accesses to the Internet, an electronic highway connecting thousands of computers and millions of individual subscribers throughout the world. It provides access to electronic mail (e-mail) communication, news from libraries and other research institutions, public domain and shareware of types, and discussion groups on a variety of topics.

With access to computers and people all over the world also comes the availability of material that may not be considered to be of educational value in the context of the school setting. The North Shore School District has taken available precautions, which are limited to filter access to objectionable materials. However, it is impossible to control access to all materials and information on the Internet.

Because we firmly believe that the valuable information and interaction available on this worldwide network far outweighs the possibility that users may procure material that is not consistent with the educational goals of the District, we have developed the following guidelines for acceptable use. In general, these guidelines require that end users (students, faculty, administrators, community members and staff) utilize the Network in an efficient, ethical and legal manner. The failure of any user to comply with the District's Acceptable Use Policy may result in disciplinary action as well as suspension and/or revocation of access privileges, and/or legal action.

A user's signature on the attached legally binding Contract Agreement and Application for a North Shore School District Internet Account indicates that the user has carefully read and fully understands this Introduction and the Terms and Conditions of Acceptable Use that follow.

North Shore School District Network – Terms and Conditions for Acceptable Use

1. A student's account can only be used to research information in support of his or her education.
2. All users must abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

- a. You must not write or send messages meant to abuse, harass, intimidate or defame others.
- b. You must use appropriate language. This means that you must not swear or use vulgarities.
- c. You must not attempt to receive, transmit or make available to others obscene, offensive or sexually explicit material.
- d. You should never reveal your personal address or telephone number, and you must never reveal the address or telephone of anyone else.
- e. You must not use the Network in any way that might disrupt the use of the Network by others. Examples of this include, but are not restricted to:
 - i. Downloading extensive files;
 - ii. Sending mass e-mail messages or transmitting or propagating chain letters;
 - iii. Annoying others by using chat functions or instant messaging unless instructed by a teacher as part of an instructional project.
- f. You must not create or spread viruses, degrade system performance, disrupt service or damage files.
- g. You must never access someone else's account. You must not use another person's email account at anytime.
- h. You must immediately notify the system administrator if you think you have identified a security problem. You must not talk about this security problem, or demonstrate it to other users.
- i. You must not attempt to login to the North Shore District Network as a system administrator.
- j. You must not vandalize any computer software, data of another user on the North Shore Network or any information connected to the North Shore Network.
- k. You must not vandalize any computer hardware, hardware peripherals, furniture or materials in any of the computer rooms, classrooms or library.
- l. You must not give out or allow the use of your personal network password(s). You must not log-on with any other password than your own.
- m. You must not change, add or delete a preference file or system file at any time.
- n. You must not attempt to gain unauthorized access to any file, resources, or computer or phone systems (including those of the District).
- o. You must not use the Network to play or download games, movies, or other forms of entertainment.

There is NO PRIVACY GUARANTEE for electronic mail (e-mail) or any use of the District Computer Network. Students, faculty, administrators, community members and staff must understand that e-mail and the Network are not guaranteed to be private and that the Network is the sole property of the District. Consequently, the system administrator may examine the account, e-mail and disks, files, etc. used in conjunction with the District Network of any user. Moreover, student violations of the Acceptable Use Policy will be immediately reported to the student's parents and may result in disciplinary action.

Use of another organization's networks or computing resources must comply with the rules of the District Network and such other network. Illegal activities are strictly prohibited. Information pertaining to or implicating illegal or unlawful 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: copyrighted material, threatening or obscene material, or material protected by trade secret. Users must respect all intellectual and property rights and laws.

In accord with the Copyright Act of 1976, a user may make "fair use" of a copyrighted work for purposes of criticism, comment, news reporting, teaching, scholarship, or research. Of course, students must always avoid plagiarism.

Use of the District Network for day-trading, on-line auctions, commercial activities by for-profit institutions, product advertisement, or for commercial gain is also prohibited.

Reliability - The North Shore School District makes no warranties of any kind, whether expressed or implied, and assumes no responsibility as to the quality, availability, or reliability of the service it is providing. Users navigate the Internet and use information at their own risk. The District will not be responsible to any user for any damages sustained or incurred in connection with the use, operation or inability to use the District Network, including, but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by the District's own negligence, errors or omissions (even where the District has been advised of the possibility of such loss), or those of the user.

The terms and conditions stated in this Policy reflect the entire agreement of the parties and supersede all prior oral or written agreements and understandings of the parties. These terms and conditions shall be governed and interpreted in accordance with the laws of the state of New York and the United States of America.

Computer Network & Internet Safety Policy 4526

COMPUTER NETWORK FOR EDUCATION

The Board of Education is committed to optimizing student learning. The Board considers student access to 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 district classrooms

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 intra-district, regional, statewide, national and global communication opportunities for staff and students.

All users of the district's computer network and the Internet must understand that use is a privilege, not a right, and that use entails responsibility.

The Superintendent of Schools shall 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 those regulations. Failure to comply may result in disciplinary action as well as suspension and/or revocation of computer access privileges.

The Superintendent shall be responsible for designating a Director of Technology to oversee the use of district computer resources. The Director of Technology will prepare in-service programs for the training and development of district staff in computer skills, and for the incorporation of computer use in appropriate subject areas.

The Director of Technology, working in conjunction with the building principals, assistant superintendents and superintendent shall develop for the Board's approval a comprehensive multiyear technology plan which shall be revised as necessary to reflect changing technology and/or district needs.

Adoption date: June 15, 2006

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.

I. Administration

The Superintendent of Schools shall designate a Director of Technology to oversee the district's computer network.

The Director of Technology shall monitor and examine all network activities, as appropriate, to ensure proper use of the system.

The Director of Technology 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 Director of Technology 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.

The Director of Technology shall ensure that all disks and software loaded onto the computer network have been scanned for computer viruses.

All student agreements to abide by district policy and regulations and parental consent forms shall be kept on file in the office of the district director of technology.

II. Internet Access

- Students will be provided access during class time; during the school day when the students are not in class; and before or after school hours
- Students will be provided with classroom accounts.
- Students may browse the World Wide Web, provided that district approved filters are operational
- Students may not participate in chat rooms.
- Students may read news groups.
- Students may not construct their own web pages using district computer resources.
- Students will have class/group e-mail address.
- Students are allowed to belong to mailing lists
- A staff member will be required to monitor all of these activities.

III. Acceptable Use and Conduct

1. A student's account can only be used to research information in support of his or her education.

2. All users must abide by the generally accepted rules of network etiquette, including but not limited to the following:

YOU MUST: immediately notify the system administrator if you think you have identified a security problem, do not show or demonstrate it to other users.

DO NOT!!!:

- a. write or send messages meant to abuse, harass, intimidate or defame others.
- b. use inappropriate language. This means that you must not swear or use vulgarities.
- c. attempt to receive, transmit or make available to others obscene, offensive or sexually explicit material.
- d. reveal your personal address or telephone number, or the address or telephone of anyone else.
- e. use the Network in any way that might disrupt the use of the Network by others. Examples of this include, but are not restricted to:
 - i. Downloading extensive files;
 - ii. Sending mass e-mail messages or transmitting or propagating chain letters;
 - iii. Annoying others by using chat functions or instant messaging unless instructed by a teacher as part of an instructional project.
- f. create or spread viruses, degrade system performance, disrupt service or damage files.
- g. access someone else's account. You must not use another person's email account at anytime.
- h. attempt to login to the North Shore District Network as a system administrator.
- i. vandalize any computer software, data of another user on the North Shore Network or any information connected to the North Shore Network.
- j. vandalize any computer hardware, hardware peripherals, furniture or materials in any of the computer rooms, classrooms or library.
- k. give out or allow the use of your personal network password(s) or log-on with any other password than your own.
- l. change, add or delete a preference file or system file at any time.
- m. attempt to gain unauthorized access to any file, resources, or computer or phone systems (including those of the District).
- n. not use the Network to play or download games, movies, or other forms of entertainment.

IV. No Privacy Guarantee

There is NO PRIVACY GUARANTEE for electronic mail (e-mail) or any use of the District Computer Network. Students, faculty, administrators, community members and staff must understand that e-mail and the Network are not guaranteed to be private and that the Network is the sole property of the district. Consequently, the system administrator may examine the account, e-mail and disks, files, etc. used in conjunction with the District Network of any user. Moreover, student violations of the Acceptable Use Policy will be immediately reported to the student's parents and may result in disciplinary action.

V. Sanctions

Use of another organization's networks or computing resources must comply with the rules of the District Network and such other network. Illegal activities are strictly prohibited. Information pertaining to or implicating illegal or unlawful 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: copyrighted material, threatening or obscene material, or material protected by trade secret. Users must respect all intellectual and property rights and laws.

In accord with the Copyright Act of 1976, a user may make "fair use" of a copyrighted work for purposes of criticism, comment, news reporting, teaching, scholarship, or research. Of course, students must always avoid plagiarism.

Use of the District Network for day-trading, on-line auctions, commercial activities by for-profit institutions, product advertisement, or for commercial gain is also prohibited.

VII. District Responsibilities

Reliability - The North Shore School District makes no warranties of any kind, whether expressed or implied, and assumes no responsibility as to the quality, availability, or reliability of the service it is providing. Users navigate the Internet and use information at their own risk. The District will not be responsible to any user for any damages sustained or incurred in connection with the use, operation or inability to use the District Network, including, but not limited to, loss of data resulting from delays, non-deliveries, misdeliveries, or service interruptions caused by the District's own negligence, errors or omissions (even where the District has been advised of the possibility of such loss), or those of the user.

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: June 15, 2006

4526.1

INTERNET SAFETY

The Board of Education is committed to undertaking efforts that serve to make safe for children the use of district computers for access to the Internet and World Wide Web. To this end, although unable to guarantee that any selected filtering and blocking technology will work perfectly, the Board directs the Superintendent of Schools to procure and implement the use of technology protection measures that block or filter Internet access by:

- adults to visual depictions that are obscene or child pornography, and
- minors to visual depictions that are obscene, child pornography, or harmful to minors, as defined in the Children's Internet Protection Act.

Subject to staff supervision, however, any such measures may be disabled or relaxed for adults conducting bona fide research or other lawful purposes, in accordance with criteria established by the Superintendent or his or her designee.

The Superintendent or his or her designee also shall develop and implement procedures that provide for the safety and security of students using electronic mail, chat rooms, and other forms of direct electronic communications; monitoring the online activities of students using district computers; and restricting student access to materials that are harmful to minors.

In addition, the Board prohibits the unauthorized disclosure, use and dissemination of personal information regarding students; unauthorized online access by students, including hacking and other unlawful activities; and access by students to inappropriate matter on the Internet and World Wide Web. The Superintendent or his or her designee shall establish and implement procedures that enforce these restrictions.

The Director of Technology designated under the district's Computer Network or Acceptable Use Policy (4526), shall monitor and examine all district computer network activities to ensure compliance with this policy and accompanying regulation. He or she also shall be responsible for ensuring that staff and students receive training on their requirements.

All users of the district's computer network, including access to the Internet and World Wide Web, must understand that use is a privilege, not a right, and that any such use entails responsibility. They must comply with the requirements of this policy and accompanying regulation, in addition to generally accepted rules of network etiquette, and the district's Acceptable Use Policy. Failure to comply may result in disciplinary action including, but not limited to, the revocation of computer access privileges.

Cross-ref: 4526, Computer Network for Education

Ref: Public Law No. 106-554

47 USC §254

20 USC §6801

Adoption date: June 15, 2006

INTERNET SAFETY REGULATION

The following rules and regulations implement the Internet Safety Policy adopted by the Board of Education to make safe for children the use of district computers for access to the Internet and World Wide Web.

Definitions

In accordance with the Children's Internet Protection Act,

Child pornography refers to any visual depiction, including any photograph, film, video, picture or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. It also includes any such visual depiction that (a) is, or appears to be, of a minor engaging in sexually explicit conduct; or (b) has been created, adapted or modified to appear that an identifiable minor is engaging in sexually explicit conduct; or (c) is advertised, promoted, presented, described, or distributed in such a manner than conveys the impression that the material is or contains a visual depiction of a minor engaging in sexually explicit conduct.

Harmful to minors means any picture, image, graphic image file, or other visual depiction that (a) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (b) 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; and (c) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Blocking and Filtering Measures

The Superintendent or his or her designee shall secure information about, and ensure the purchase or provision of, a technology protection measure that blocks access from all district computers to visual depictions on the Internet and World Wide Web that are obscene, child pornography or harmful to minors.

The district's Director of Technology shall be responsible for ensuring the installation and proper use of any Internet blocking and filtering technology protection measure obtained by the district.

The Director of Technology or his or her designee may disable or relax the district's Internet blocking and filtering technology measure only for adult staff members conducting research related to the discharge of their official responsibilities.

The Director of Technology shall monitor the online activities of adult staff members for whom the blocking and filtering technology measure has been disabled or relaxed to ensure there is not access to visual depictions that are obscene or child pornography.

Monitoring of Online Activities

The district's Director of Technology shall be responsible for monitoring to ensure that the online activities of staff and students are consistent with the district's Internet Safety Policy and this regulation. He or she may inspect, copy, review, and store at any time, and without prior notice, any and all usage of the district's computer network for accessing the Internet and World Wide Web and direct electronic communications, as well as any and all information transmitted or received during such use. All users of the district's computer network shall have no expectation of privacy regarding any such materials.

Except as otherwise authorized under the district's Computer Network or Acceptable Use Policy, students may use the district's computer network to access the Internet and World Wide Web only during supervised class time, study periods or at the school library, and exclusively for research related to their course work.

Staff supervising students using district computers shall help to monitor student online activities to ensure students access the Internet and World Wide Web, and/or participate in authorized forms of direct electronic communications in accordance with the district's Internet Safety Policy and this regulation.

The district's Director of Technology shall monitor student online activities to ensure students are not engaging in hacking (gaining or attempting to gain unauthorized access to other computers or computer systems), and other unlawful activities.

Training

The district's Director of Technology shall provide training to staff and students on the requirements of the Internet Safety Policy and this regulation at the beginning of each school year.

The training of staff and students shall highlight the various activities prohibited by the Internet Safety Policy, and the responsibility of staff to monitor student online activities to ensure compliance therewith. Students shall be directed to consult with their classroom teacher if they are unsure whether their contemplated activities when accessing the Internet or Worldwide Web are directly related to their course work.

Staff and students will be advised to not disclose, use and disseminate personal information about students when accessing the Internet or engaging in authorized forms of direct electronic communications.

Staff and students will also be informed of the range of possible consequences attendant to a violation of the Internet Safety Policy and this regulation.

Reporting of Violations

Violations of the Internet Safety Policy and this regulation by students and staff shall be reported to the Building Principal.

The Principal shall take appropriate corrective action in accordance with authorized disciplinary procedures.

Penalties may include, but are not limited to, the revocation of computer access privileges, as well as school suspension in the case of students and disciplinary charges in the case of teachers.

Adoption date: June 15, 2006

ACCOUNTABILITY FOR SCHOOL PROPERTY

Students are issued various materials throughout the year (textbooks, calculators, digital mobile devices, etc.) for which they are held responsible. In the event that any of the materials are destroyed, defaced or lost, the student will be issued an accountability slip – that is, a requirement to pay an amount of money in lieu of the material issued. Destruction or defacement of school property in any form will result in serious disciplinary action. Should materials become lost during the school year, the student is to report this to his/her teacher and make arrangements to pay for the replacement. Students who owe an accountability will be unable to attend any formal social function (i.e. sports night, prom, etc.) until it is paid. In the case of seniors, caps and gowns for graduation will not be issued until all accountabilities are settled by the student.

Adopted: February 17, 2011

Revised: January 17, 2013

CHROMEBOOK PROTECTION PLAN

Please review the entire Chromebook Student Handbook prior to completing this form. The most recent version may be found at <https://northshoreschools.org/chrome>

Date: _____

Grade Level: _____

Parent Name (Please Print): _____

Parent Signature: _____

Student Name (Please Print): _____

Required attachment: \$50.00 check or money order payable to North Shore Schools

You agree to pay the District a non-refundable fee of \$50.00 for a non-transferrable protection plan that provides full coverage of theft, loss, or damage to one District-issued Chromebook. This Protection Plan is valid only for the Chromebook that is assigned to the student and will be in effect across all school years and extended breaks until the Chromebook becomes damaged or lost/stolen.

In cases of theft, vandalism and other criminal acts, a police report MUST be filed by the student or parent for the protection coverage to take place. Reports may be filed at the Third Police Precinct (214 Hillside Ave, Williston Park 11596). A copy of the police report must be provided to Central Office.

Protection plans do NOT cover the loss of any Chromebook accessories (power adapters, protective sleeves). Any attempt to repair the Chromebook with a third-party service will result in the nullification of the protection plan, and parents will assume the full cost of replacement (\$299).

IMPORTANT: Students who graduate, withdraw, are expelled, or terminate enrollment within the North Shore Schools for any other reason must return his or her individual school Chromebook to the Technology Office on or before the date of departure from the District. Protection Plans cannot be applied towards a missing Chromebook in this circumstance without an accompanying copy of a filed police report.

Please send this completed form with accompanying payment and any additional documentation (AUP, student pledge) as required by your selected option to:

**North Shore CSD
Attn: Lois Straber
112 Franklin Avenue
Sea Cliff, NY 11579**

NORTH SHORE CENTRAL SCHOOL DISTRICT
CHROMEBOOK MEMORANDUM OF UNDERSTANDING

By signing this Memorandum of Understanding, you and your child agree to accept all policies and procedures set forth in the Chromebook Student Handbook (<https://www.northshoreschools.org/chrome>), as well as all related documents including the Chromebook Protection Plan and the District Acceptable Use Policy. The District will not issue a Chromebook to your child without consent to this Memorandum of Understanding.

I have reviewed, understand, and agree to comply with the above stipulations.

Date: _____ Grade Level: _____

Parent Name (Please Print): _____

Parent Signature: _____

Student Name (Please Print): _____

Please send this completed form to:

North Shore CSD
Attn: Lois Straber
112 Franklin Avenue
Sea Cliff, NY 11579

NORTH SHORE CENTRAL SCHOOL DISTRICT
STUDENT AUP AGREEMENT

I have read the North Shore School District Computer Network Introduction and the Terms and Conditions for Acceptable Use. I fully understand and will abide by the stated Terms and Conditions for the North Shore School District Computer Network. I understand that there is no privacy guarantee for e-mail or any use of the District Network.

I further understand that any violation of this Policy may result in disciplinary action and suspension and/or revocation of access privileges and/or legal action. Moreover, I am legally responsible for any action I take with regard to use of the Network and any evidence of violation of federal, state and/or local law will be forwarded to the proper authorities.

In consideration for the privilege of using the North Shore School District Computer Network, on behalf of myself, and my respective relatives, heirs, estates, and assigns, I hereby release and discharge the North Shore School District, and its respective officers, employees and agents, from any and all claims and liabilities arising out of or resulting from any use, operation, or inability to use the District Network. I further agree to defend and indemnify the District and hold the District harmless from and against any and all claims, proceedings, damages, injuries, liabilities, losses, costs, and expenses (including reasonable attorneys' fees) relating to any acts taken by me or material or information transmitted by me in connection with any use of the District Network.

Student Name (Please Print): _____

Student Signature: _____

Date: _____

Please send this completed form to:

North Shore CSD
Attn: Lois Straber
112 Franklin Avenue
Sea Cliff, NY 11579

NORTH SHORE CENTRAL SCHOOL DISTRICT
PARENT AUP AGREEMENT

As the parent or guardian of this student, I have read and fully understand the Introduction and the Terms and Conditions for Acceptable Technology Use in the North Shore School District Network. I understand that this access is designed for educational purposes only and have fully discussed this fact with my child. I assume responsibility for the content of messages transmitted or posted by my child.

I understand that although the North Shore School District has taken precautions to eliminate objectionable material, it is impossible for the North Shore School District to restrict all access to objectionable materials. I hereby give my permission to issue an account for my child and certify that the information contained on this form is correct. I understand that I am financially responsible for any and all charges made by my child to his or her account.

Finally, in consideration for my child’s use of the District Network, on behalf of myself and my child, and our respective relatives, heirs, estates and assigns, I hereby release and discharge the North Shore School District, and its respective officers, employees and agents, for any and all claims and liabilities arising out of or resulting from my child’s use, operation or inability to use the District Network. I further agree to defend and indemnify the District and hold the District harmless from and against any and all claims, proceedings, damages, injuries, liabilities, losses, costs, and expenses (including reasonable attorney’s fees) relating to any acts taken by my child or material or information transmitted by my child in connection with any use of the District Network.

Parent or Guardian Name (Please Print): _____

Parent or Guardian Signature: _____

Date: _____

Please send this completed form to:

North Shore CSD
Attn: Lois Straber
112 Franklin Avenue
Sea Cliff, NY 11579