

Table Of Contents

[ACCEPTABLE USE POLICY- August 2022](#)

[USE OF PERSONAL DEVICES ON THE NETWORK POLICY-APRIL 2021](#)

NORTHVIEW PUBLIC SCHOOLS’ ACCEPTABLE USE POLICY- Updated August 2022 (herein referred to as the AUP)

OVERVIEW

Northview Public Schools provides its students, staff, and community access to a multitude of technology resources. These resources provide opportunities to enhance learning and improve communication within our community and with the global community beyond our campus. With the privilege of access is the responsibility of exercising appropriate personal responsibility in the use of these resources. The Northview Public School policies are intended to promote the most effective, safe, productive, and instructionally sound uses of networked information & communication tools. Northview Public Schools also makes a good faith effort to protect its students and users from exposure to Internet materials that are harmful or explicit. The Technology Department maintains an Internet content filtering device and software controls to meet federal standards established in the Children’s Internet Protection Act (CIPA).

EXPECTATIONS

Responsible use of district technology resources is expected to be ethical, respectful, academically honest, and supportive of the district’s mission. Each computer user has a responsibility to respect every other person in our community and on the Internet. Digital storage and electronic devices that access the network will be treated as extensions of the physical school space. Administrators, or their designees, may review files and communications (including, but not limited to electronic mail) to ensure that users are using the system in accordance with district policy. The district may also use tools to remote into school owned devices. (eg. chrome remote desktop). Users should not expect that files stored on servers or disks will be private. Users also should understand that school servers regularly record electronic activity in log files. Staff are required to abide by the Staff AUP in addition to what is set forth in this document.

Some activities are expressly prohibited by law. Users are expected to abide by the generally accepted rules of network etiquette. The following guidelines are intended to clarify expectations for conduct, but they should not be construed as all-inclusive.

- Use of electronic devices are to be consistent with the district’s educational objectives, mission and curriculum.

- Transmission of any material in violation of any local, federal and state laws is prohibited. This includes, but is not limited to: copyrighted material, licensed material and threatening or obscene material.
- Intentional use of computing resources to access proxy sites, pornographic material, explicit text or files, or files dangerous to the integrity of the network is strictly prohibited.
- Intentional use of any product or device to circumvent content filtering and/or network security including but not limited to VPNs or proxies is strictly prohibited.
- Software and/or services may not be installed or downloaded on school devices without prior approval of the Director of Technology or designee.
- Use of computing resources for commercial activities, product advertisement or religious or political lobbying is prohibited.
- Users may be held personally and financially responsible for malicious or intentional damage done to network software, data, user accounts, hardware and/or unauthorized costs that may be incurred.
- Files stored on any district-managed network or service are the property of the school district and, as such, may be inspected at any time and should not be considered private.
- Materials published for electronic publication must be for educational purposes. School administrators, teachers and staff may monitor these materials to ensure compliance with content standards.

VIOLATIONS

The school reserves the right to refuse access to electronic resources to anyone. Violating any portion of this policy may result in disciplinary action, including temporary or permanent ban on computer or internet use, suspension or dismissal from school, and/or legal action. Northview Public Schools may cooperate with law enforcement officers in investigations related to illegal activities conducted through its network.

LIMITATIONS

Northview Public schools implements precautions to avoid inappropriate material however no filter is 100% full proof and it is impossible to eliminate all potential access to controversial materials. By using the network or granting permission to one's child to use the network, parents and guardians agree to not hold Northview Public Schools responsible for materials acquired on the network/Internet.

USE OF PERSONAL DEVICES ON THE NETWORK POLICY-APRIL 2021

Personal network devices (phones, tablets, laptops, etc.) may be used in Northview Public Schools in accordance with the following policy. This policy is designed to protect the guest and the Northview Public Schools Network. Network access is available through the guest wireless network and may be accessed by any wireless device. The guest wireless network provides filtered Internet access and related web-based services only.

Each time someone accesses the guest wireless network they agree to the [Northview Public Schools' acceptable use policy](#) as well as the terms listed below. If you wish to use the guest wireless network at Northview Public Schools, please familiarize yourself with the information below.

- Personal network devices include any privately owned networkable electronic device connected to any Northview managed network.
- Northview Public Schools will not be held liable for any damage that may occur as a result of connecting to the guest wireless network or any electrical power source.
- Northview Public Schools will not be held responsible for any damage, loss or theft of the personal network device.
- The guest wireless network is provided as is with no warranty as to usability for a particular purpose. Northview Public Schools will not be held liable for any disruption of service.
- Northview Public Schools reserves the right to disconnect any personal network device from the network for any reason without notice in order to protect the integrity of the Northview Public Schools Network and/or to preserve the mission of the organization. Northview Public Schools also reserves the right to log any personal network device content and/or activity while the device is connected to the guest wireless network.
- Guest wireless network access is provided for filtered Internet access and related web-based services only. Personal network devices will not be allowed access to other Northview related systems such as printers, servers, user files, or user home directories.
- Personal network devices may be connected exclusively to the guest wireless network in Northview Public School buildings in the areas where this coverage is available. They are not permitted to be connected to any hardwired connections.
- Illegal, destructive, harmful, or any other inappropriate activities including but not limited to computer hacking, harassment, accessing offensive/obscene materials, or engaging in illegal activities are strictly prohibited.

- The owner of the device is exclusively responsible for how the device is used. The owner is responsible for the security of the device, including but not limited to having the latest security patches for its operating system installed and must be running anti-virus software with the latest virus definition files.
- The owner of the device is exclusively responsible for the configuration of the device. This includes network configuration. Northview Public Schools is not responsible for providing technical support for personal network devices.
- Student use of personal network devices in the classroom setting will be at the discretion of the classroom teacher.
- The device must not interfere with the normal function of Northview Public Schools' Network or other wireless devices. If interference occurs, the device may be disallowed from accessing the network.
- No mobile device may be used as a portable Wi-fi hotspot while on school grounds.
- The device must be free of spyware, adware, worms, viruses, Trojan horses, and peer-to-peer software.
- The device must be used as a client only and may not run server related services including but not limited to web hosting services, email services, or proxy services.
- The owner of the device, or in the case of a student their parents and/or guardians, agrees to be responsible for and to reimburse Northview Public Schools for any damage that may be caused by the personal network device or use thereof while connected to the guest wireless network.

Agreement to the Acceptable Use Policy

By clicking submit, (or signing below), I certify that I have read and agree to the Terms and Conditions listed in the [Northview Public Schools' Acceptable Use Policy](#) which complement [Board Policies](#) 7530,7540,7542 and 7543. I understand and will abide by the Terms and Conditions for Network and Internet Access. I further understand that any violation of the regulations is unethical and may constitute a criminal offense. Should I commit any violation, my access privileges may be revoked, school disciplinary action may be taken and/or appropriate legal action.

_____ (Printed Name) _____ (Signature)

_____ (Date)