

<p style="text-align: center;">North Providence School Department Computer/Technology Resources Authorized User Policy</p>	<p style="text-align: center;">Approved: 5/27/2020</p>

NORTH PROVIDENCE SCHOOL DISTRICT
COMPUTER / TECHNOLOGY RESOURCES
AUTHORIZED USER POLICY

Adopted 2020
Supersedes- Acceptable uses of the district computer
network and the internet- Staff Policy approved 9-26-12

SECTION 1: INTRODUCTION

The North Providence School District recognizes the need for computers, electronic communications, and Internet access systems and the vital role they play in assisting District employees and other authorized users in providing numerous public services for education. The District provides computers, electronic communications, and Internet access systems as tools that will assist employees in providing these services as part of their daily functions. Be advised that if the District or its Communications Department staff discovers evidence of misuse, illegal activity, or any activity that violates any of the District policies and procedures, or an individual school technology policy, the District may consider appropriate corrective action, discipline, and/or disclosure of evidence to law enforcement officials.

All information and communication on the District technology system is the property of the North Providence School District and there is no expectation of privacy.

While respecting the privacy of our authorized users, the North Providence School District is also concerned with protecting and securing itself and its computerized information. The District needs to maintain a high level of professionalism and therefore needs to monitor and manage the use of its resources in a manner that will maximize business and educational operations. All policies and procedures pertaining to the District networks and devices shall be described in its "North Providence School Districts Information Security Policy" that is located on the District Web-site and on hard copy held by Human Resources for distribution to new employees of the district.

SECTION 2: POLICY

2.1 This policy is applicable to all authorized users that have access to a District owned or sponsored computer, software, and network facilities which consequently may have access to electronic mail, online services, and the use of shared folders and documents.

2.2 The purpose of this policy is to define the rules of conduct and behavior of all North Providence School District authorized users when utilizing the District electronic communications (email), Internet, phone, and network systems. The rules apply to access of the District technology resources at any location, from any device, via wired or wireless connection.

2.3 Certain approved users may be assigned to open or restricted Internet access where such access is essential to the performance of that user's duties.

2.4 Request for Internet access to sites that are blocked by the District for educational purposes shall request approval following the District's approved "School Internet Content Filtering Policy" posted on the District website. Access for staff members' related activity for an approved user must be done in writing by the approved user's Principal or Department Chair to the Director of Communications.

2.5 The provisions of this policy shall apply to the whole of the District, its District associates and all authorized users utilizing any District provided computer, software, network service, or any other school District information system or service.

2.6 All users are reminded that electronic communications and Internet access is subject to all applicable Federal, State and local laws, regulations, ordinances, or policies.

2.7 Authorized users are responsible for observing copyright and licensing agreements that may apply when downloading files, documents, and software.

2.8 The provisions of this policy shall apply to the whole of the District, its District associates and employees, and to any vendor and/or contractor or consultant utilizing any District provided Wi-Fi, computers, including laptops, MDT's, either on or off district premises, during or outside of normal working hours.

2.9 All email, electronic, and/or phone correspondence sent and received by District employees for:

- ***All School Department business***
- ***All correspondence between District employees and students***
- ***All correspondence between District employees and parents or guardians***
- ***All correspondence between District employees and medical professionals.***
- ***All correspondence between District employees and any Federal, State, and local officials***

SHALL BE DONE USING THEIR DISTRICT PROVIDED EMAIL ACCOUNT

At no time shall an employee use a personal Email account or phone to conduct any District business listed above

SECTION 3: SCOPE

3.1 The following policies define appropriate use of the North Providence School District network, computers, mobile computing devices, smart phones, all related peripherals, software, electronic communications, and Internet access.

3.2 The policies apply to all users of District technology resources regardless of employment status.

3.3 The District authorizes the use of their computing and network resources to any authorized user to carry out legitimate school business.

3.4 All authorized users of District computing and network resources will do so in an ethical, legal, and responsible manner.

SECTION 4: DEFINITIONS

4.1 ACCESS: means to instruct, communicate with, store data in, or retrieve data from a computer, computer system or computer network.

4.2 APPLICATION PASSWORD: a password that a user may assign within an application and/or document in a district computer that prohibits other users from opening the secured application or document.

4.3 AUTHORIZED SOFTWARE: means computer software developed, approved, purchased or licensed by an agency of the North Providence School District.

4.4 AUTHORIZED USER: includes all school employees including full-time, part-time, temporary, contract employees, teachers, teacher assistants, student teachers, teacher aids, psychiatrists, therapists, councilors, custodians, food service personnel, volunteers, students or interns, elected officials, and other authorized organizations or individuals that the District has given the approval to utilize its computers and technology systems.

4.5 COMPUTER: all computing hardware and operating systems.

4.6 COMPUTER NETWORK: means either a set of related devices connected to a computer by communications facilities, or a complex of two or more computers, including related devices, connected by communications facilities.

4.7 COMPUTER SOFTWARE: means one or more computer programs, existing in any form, instructions, manuals, associated operational procedures, or other documentation. Software provides the instructions and controls through symbolic languages of the operation of all computers, including stand-alone and LAN (local area network) computers and related equipment as well as midrange computers.

4.8 COMPUTER SYSTEM: means one or more connected or unconnected computers, peripheral devices, software, data, programs, communications facilities, and computer networks.

4.9 COPYRIGHT: means the right granted to the owner of software by the Copyright Act, Title 17 of the U.S Code.

4.10 DIRECTORY: a directory is a named group of related files that are separated by the naming convention from other groups of files.

4.11 DOCUMENT: is a piece of work created with an application such as by a word processor. A computer file that contains data for use by applications.

4.12 ELECTRONIC MAIL (E-MAIL): refers to the electronic transfer of information typically in the form of an electronic message, memoranda and attached documents from a sending party to one or more receiving parties via an immediate telecommunications system. Electronic mail is a means of sending messages between computers using a computer network. Electronic mail services not only consist of the use of district-provided electronic mail systems but also the act of sending and/or receiving electronic mail across the Internet.

4.13 EMPLOYEE: the term employee shall include but not be limited to any school employees including full-time, part-time, temporary, contract employees, teachers, teacher assistance, student teachers, teacher aids, psychiatrists, therapists, councilors, custodians, food service personnel, volunteers, students or interns, elected officials and other authorized organizations or individuals. Also known as a "User"

4.14 INTERNET SERVICE PROVIDER: an entity that provides the initial host connection to the Internet.

4.15 FILE: A file is an entity of data. Files can be program files, which contains instructions that allow the computer to perform various tasks under the control of the user, or data files, that contain information only. The file must have a unique name within its own directory.

4.16 FOLDER: is a location that stores multiple files and is used to organize information.

4.17 INTERNET: The worldwide network of networks connected to each other using the IP protocol and other similar protocols. The Internet enables a variety of information management services, including, but not limited to, e-mail, instant messaging, file transfers, file uploads, file downloads, news, and other services.

4.18 LAN: means Local Area Network or a system served by one or more file servers.

4.19 LICENSE AGREEMENT: means a contract between the software publisher and the intended user.

4.20 LOG-IN NAME: is the unique account name assigned a user to access a computer system, also known as user-ID or user name.

4.21 LOG-IN PASSWORD: a unique code word linked to the log-in name that is used by an individual employee to gain access to a computer resource.

4.22 NETWORK OPERATION: logging onto or using a work station, application, or program linked to or installed on a file server.

4.23 SYSTEM ADMINISTRATOR: Person(s) responsible for the operation and maintenance of all software, workstations, file servers and peripheral equipment (may also be referred to as the Information Technology Technician).

4.24 USER: The term USER shall include but not be limited to any school employees including full-time, part-time, temporary, contract employees, teachers, teacher assistance, student teachers, teacher aids, psychiatrists, therapists, councilors, custodians, food service personnel, volunteers, students or interns, elected officials and other authorized organizations or individuals, who utilize the District information assets and technology.

4.25 VIRUS: a computer generated message used to debilitate, destroy, or disrupt the proper functioning of a computer system.

4.26 WORKSTATION: All computer-related hardware, including but not limited to, processor, keyboard, monitor, printer, mouse, track-balls, scanners, digital imaging devices, modems, UPS devices, surge protectors, cables, connectors, adapters, telephones, and any other device attached to any component.

SECTION 5: OWNERSHIP OF DATA - COMPUTER & NETWORK PRIVACY ISSUES

5.1 The North Providence School District owns all data, files, information and communications created on, stored on, transmitted, received or exchanged via its network, communications systems, equipment and devices (including email, voicemail, text messages, and Internet usage logs).

Data contained on all networks and computers. The District reserves the right to inspect and monitor any and all such communications at any time, for any purpose, and with or without notice to any authorized user.

Users must keep in mind that any electronic communications and Internet usage on district equipment and software, by law, may be subject to the RI Public Information Law.

5.2 All authorized users are reminded that electronic communications and Internet access is subject to all applicable Federal, State and local laws, regulations, ordinances, or policies. Authorized users are responsible for observing copyright and licensing agreements that may apply when downloading files, documents and software, which includes the cutting and pasting of a document and videos used for educational purposes.

5.3 The District holds no responsibility or accountability for any personal data that was created on, downloaded to, or copied to a District owned computer device or network device.

SECTION 6: SYSTEM ADMINISTRATION

6.1 The Director of Communications shall be the administrator of the District computer system and technology resources. He/she shall have the responsibility for all District computer hardware software and data resources. The terms "Department of Communications" & "Information Technology Department" are used interchangeably. The Director of Communications will assign Communications Department personnel to assist him/her in performing the required functions of the Department such as an Assistant Director, System Administrator, Network Administrator, Data Manager, or Technicians.

SECTION 7: PROCUREMENT PROCESS

7.1 All procurement requests for computer hardware or software must be forwarded to the Director of Communications / Information Technology Department, for review and approval. This is required to ensure appropriate standardization of products and technology.

SECTION 8: MOVING / INSTALLATION EQUIPMENT OR SOFTWARE

8.1 All equipment shall be moved or assembled by the Communications Department.

8.2 Any peripheral equipment shall be installed and attached by the Communications Department.

8.3 The installation or deletion of any software on any district computer and/or file servers shall be installed or removed by the Communications Department.

8.4 No user shall ever plug any cord or device into a district network outlet or infrastructure under any circumstances.

SECTION 9: PERSONAL USE OF DISTRICT WI-FI/ COMPUTER / TECHNOLOGY RESOURCES

9.1 The District computers and technology resources can be used for incidental, brief and occasional personal needs as long as use does not result in or subject the district to any additional cost, liability or user loss of productivity. It shall be up to each Department Head or Principal to set rules and regulations, standard operating procedures, or department polices pertaining to personnel use.

9.2 The personal use of a District computer and its technology resources can only be performed during the authorized user's designated duty-free times, lunch times, or off-duty times.

9.3 Personal use of technology cannot interfere with business, student education, productivity, performance, or; pose additional risk to security, reliability or privacy.

9.4 Personal use of technology cannot cause conflict with any district policy or work rule.

9.5 Users are prohibited from downloading personal or non-work related information such as pictures, videos, and audio on a District owned computer or its technology resources, unless specifically authorized by the Communications Department.

9.6 The use of the District computers or its technology to transmit or download any material that is discriminatory, defamatory, harassing, insulting, offensive, pornographic, or obscene is prohibited.

9.7 Failure to adhere to any part(s) of this policy may result in loss of computer rights or other disciplinary actions (in accordance with district-wide or individual departments SOP's, and user's respective Collective Bargaining Agreement).

9.8 All users are reminded that electronic communications and Internet access is subject to all applicable Federal, State and local laws, regulations, ordinances or policies. All approved users are responsible for observing copyright and licensing agreements that may apply when downloading files, documents or software.

9.9 This document does NOT attempt to address every possible situation that may arise. Professional judgment, etiquette and common sense should be exercised while using district technology resources.

SECTION 10: INTERNET USAGE AND MISUSE:

10.1 This technology usage policy outlines appropriate and inappropriate use of the Internet. Usage shall be focused on business or educational related tasks.

10.2 Use of the Internet, as with all technology resources, shall conform to all District policies and work rules.

There are numerous acceptable and appropriate uses of the District computers and its technology systems such as:

- ***Participating in professional, work-related research***
- ***The purpose of education to students***
- ***Distributing work-related correspondence, minutes, agendas and reports.***
- ***Responding to public inquiries.***
- ***Creating work-related information resources.***
- ***Participating in work-related mailing lists or forums.***
- ***Communicating with staff, elected officials and appropriate outside bodies.***

Filtering software will be used by the district to preclude access to inappropriate web sites unless specific exemptions are granted as a requirement of work duties.

- ***Visiting or otherwise accessing the following types of sites is prohibited:***
- ***Adult, sexually-oriented or other offensive web sites***
- ***Sites associated with hate crimes or violence***
- ***Personal dating or chat room sites***
- ***Gambling sites***
- ***Sites that would create discomfort to a reasonable person in the workplace***
- ***Use of district computer or its technology resources to solicit or purchase any products or services that are unrelated to district business or educational purposes.***
- ***Use of district computer or its technology to engage in private or business activities, including excessive use of instant messaging and chat rooms.***
- ***Use of Drop Box, Sky Drive or any similar site for the transfer of files is prohibited unless authorized by the Director of Communications.***
- ***Use of remote desktop software such as Log-Me-In, Go-To-My-PC or any similar site or software is prohibited unless authorized by the Director of Communications.***
- ***Use of district computer or its technology resources for personal business or gain.***
- ***Use of district computer or its technology for political, religious or benevolent association activity purposes.***
- ***Use of district computer or its technology resources for illegal, harassing or malicious purposes***
- ***Use of district computer or its technology to send or post chain letters, ponzi or other pyramid schemes of any type.***
- ***Use of district computer or its technology to transmit or download any material that is discriminatory, defamatory, harassing, insulting, offensive, pornographic or obscene.***
- ***Use of district computer or its technology to broadcast network wide non-business related e-mails is prohibited.***
- ***Use of the district computer or its technology for unauthorized access into for-pay sites.***

- ***Use of the district computer or its technology for union business, other than by the Human Resources Department and Union officials is prohibited. Exception may be when district and Union agree to permit such usage.***
- ***Deliberately propagating any virus, worm or other code or file to disrupt, disable, impair, or otherwise harm the district's systems is prohibited.***
- ***Accessing networks, servers, drives, folders or files to which an authorized user has not been granted access is prohibited.***
- ***Making unauthorized copies of district files or other district data is prohibited.***
- ***Attempting to circumvent prohibitions is a violation of this policy.***

Any authorized user of the District technology resources that accidentally visits any of the sites that are prohibited under this policy shall immediately notify his/her supervisor, Principal, or administrator and then the Communications Director.

Vandalizing any hardware, software, computer, electronic communications, or Internet access is prohibited.

Authorized users shall not send, transmit or otherwise disseminate non-public personal data, or confidential information of the district to an unauthorized person or in an unauthorized manner.

Privately owned computer systems, laptop computers or peripherals may only be added to the districts technology system by a member of the Communications Department and is subject to the districts "Information Security Policy"

The North Providence School District prohibits the dissemination of any District owned or shared information, in any form, contained in or accessed through the district's computers, to any other person except one who is officially entitled to receive such information, without having approval of either the specific Department Head, Principal, Administrator and/or the Communications Department Staff.

The use of personal picture for the use of "Wall-paper" or background scenes are permitted but must be approved by the department head or Principal. No wall paper or background picture should be offensive in nature and disrupt other employees or visitors with view of the screen.

This list is not all inclusive and does not attempt to address every situation that may arise. Professional judgment, etiquette and common sense should be exercised while using district technology resources.

SECTION 11: COMPUTER SOFTWARE

11.1 Illegal or unauthorized use of software may have severe consequences, including legal action for an injunction barring further use of the software and actions for monetary damages and penalties.

11.2 In most cases, the district does not own the rights to software developed by a third party. Instead the District rights are governed exclusively by a license agreement. Unless expressly authorized by the license agreement, the district does not have the right to reproduce either the software or its related documentation. It is the policy of the District to respect all computer software copyrights and to adhere to the terms of all software licenses to which all employees, and other approved users are a party. The District prohibits the illegal duplication or use of computer software, whether developed by its own employees or by a third party.

11.3 Each authorized user using original issue, commercial copyrighted software shall do so only in accordance with the applicable license agreement and departmental policy. Town or District proprietary software is to be used only to conduct the District business and is not to be copied for personal use or transferred to third parties without administrative authorization and without execution of appropriate licensing documentation.

11.4 Any authorized user learning of any misuse of software or related documentation or have questions pertaining to said same should contact the Communications Director.

SECTION 12: USE AND CARE OF EQUIPMENT

12.1 Authorized users are reminded that the districts workstations and mobile devices are of vital importance to the productivity of the district and educational purposes. These costly and environmentally sensitive electrical devices require proper use and care. Therefore, employees shall adhere to the following guidelines to ensure the equipment is handled with due care:

- ***Do not expose any equipment or components to liquid, dust, heat, shock or magnetic influence nor permit the accumulations of materials likely to restrict the systems ventilation.***
- ***Do not unplug workstations from surge protectors or UPS devices.***
- ***Do not plug in any unauthorized electronic devices into a surge protector or UPS device.***
- ***Do not unplug, reconfigure or move computer components from their original location without prior approval from the Communications Department.***
- ***Notify your supervisor, principal, or department head of damage or equipment malfunctions involving any workstations, laptops, or mobile devices. Supervisors, principals, or department heads will notify the Communications Department personnel via a work order.***

SECTION 13: SYSTEM MONITORING

13.1 All authorized users should be aware that the District computers and network services create activity records, including but not limited to, every Internet site visited and every email message sent and received.

13.2 The Communications Department/ Information Technology Department is responsible for the periodic monitoring and auditing of the entire districts technology system.

13.3 The District, in its discretion, reserves the right to monitor usage for Internet communications and contents of e-mail messages to insure no unauthorized or illegal use is occurring.

13.4 The District reserves the right to selectively restrict user access to certain hardware and software.

13.5 The District reserves the right to install security measures such as passwords and/or selectively restrict access to relevant parts of the network only.

13.6 The District reserves the right to disable access to certain Internet protocols and sites. Also to install software to screen out access to undesirable web sites.

13.7 The District reserves the right to install software to track or monitor e-mail and/or Internet usage.

13.8 The electronic communications system is North Providence School District property. All messages composed, sent or received on the electronic mail system are and remain the property of the district. The messages are not the private property of the user. The confidentiality of any message should not be assumed.

13.9 Any employees learning of or suspecting misuse of the District computer resources, including its hardware, software, related documentation, mobile data, or Requests for Electronic Data should notify the Director of Communications.

13.10 The Department of Communications reserves the right to request users' names with associated passwords on its networks to be able to maintain access control and ability to assist end users in solving problems. Network, Email address passwords, or application passwords will not be stored by the Communications Department.

SECTION 14: SECURITY MEASURES

14.1 Security measures must be in place to protect the network and its users. This section is governed by the district "North Providence School District Information Security Policy" that is a separate document required by law and shall be referenced to as part of this policy.

SECTION 15: VIOLATIONS / DISCIPLINARY ACTIONS

15.1 Any violation of any of the provisions of this policy can lead to loss of computer services and/or progressive disciplinary action in accordance with the user's respective administrative SOP's, rules and or regulations, and their Collective Bargaining Agreement.

15.2 It is a violation of this policy for any authorized user, including system administrators and supervisors, to access electronic mail and computer systems files to satisfy curiosity about the affairs of others.

Fist Read: 2/26/2020
Second Read:
Third Read:

NORTH PROVIDENCE SCHOOL DISTRICT
COMPUTER / TECHNOLOGY RESOURCES
AUTHORIZED USER POLICY

By signing below, I hereby acknowledge that I have received and read a copy of the “North Providence School District Computer / Technology Resources Use Policy,” and I agree to adhere to the contents of this policy. I have been afforded an opportunity to discuss and resolve any questions relative to the contents of this policy and will be provided instruction on the requirements set forth in this policy by a Communications Department / Information Technology Department staff member.

Read, understood and acknowledged by:

Signature of Authorized User

Printed Authorized User Name

Date

Witnessed by:

Signature of witness

Fist Read: 2/26/2020
Second Read: 4/29/2020
Third Read/Approved: 5/27/2020