North Providence School Department Information Security Policy	**Approved: 5/27/2020**

Introduction:

This document, the Information Security Policy (Policy), defines the governing principles for the secure operation and management of the information technology used, administered, and/or maintained by the North Providence School District and for the protection of the districts information assets.

Violations of the North Providence School District Information Security Policy must be reported to Director of Communications, building principal (if applicable) and the Superintendent.

Section 1: Purpose

1.1 To define the responsibilities of the School District employees, agents, departments, boards, School Committee persons, and agencies with respect to appropriate use and protection of the school district information assets and technology.

1.2. To ensure that the North Providence School District information assets and technology are secure from unauthorized access, misuse, degradation, or destruction.

Section 2: Scope

2.1. This Information Security Policy applies to the North Providence School District, its administration departments, school committee members, boards, offices, and agencies, employees (including but not limited to teachers, substitute teachers, teacher assistances, custodians, building maintenance staff, councilors, therapists, psychiatrists, temporary employees, interns, vendors, consultants, contractors and agents thereof--collectively referred to as —User(s).

2.2. The principles set forth in this policy are applicable to all information technology and assets, in all formats, used by personnel working in the North Providence School District.

2.3 This policy details certain purposes, procedures, guidelines, responsibilities, and other matters the North Providence School District deems relevant to its management of information assets. This policy is a living document and the District reserves the right to amend this policy or any part or provision of it on a regular bases or as deemed necessary to protect an immediate known treat to its equipment or data.

Section 3: Definitions

All employees should be familiar with the definitions in appendix A as part of their understanding of this Information Security Policy.

Section 4: Organizing Information Security

4.1 Information Security Co-ordination

The Department of Public Safety Communications Department is responsible for designing, implementing, and maintaining a district-wide information security program--in conjunction with other departments--and for assisting all school departments, town departments, agencies and maintaining information management practices at their respective locations.

4.2 Allocation of information security responsibilities

The Director of Communications is responsible for overall security of information assets and technology in the school district. The Director may delegate specific responsibilities related to information security to others within the town/school department based on their job function.

4.3 Confidentiality Agreements

Employees, consultants, or contractors who use the schools' information technology are required to read, understand, and agree to the District computer use policy regarding their responsibilities and conduct related to the protection of the District information assets and technology.

4.4 Third Parties

The School District often utilizes third parties in support of delivering business and educational services. When, as a result, these arrangements extend the District information technology enterprise or business processes into the third parties computing environments—for example, in cases of Application Service Providers (ASPs)—the third parties must abide by this Policy, as applicable, unless specific additional provisions have been established through contractual agreements.

Outside business services may also be known as

- ***Vendors***
- ***Temp agency Employees***
- ***Contractors***
- ***Subs***

Anyone listed above is also required to provide an "Insurance Bond" for any and all employees that are assigned to the North Providence School District that need access to computers or network systems. This coverage is required in the amount of $300,000.00 in the event any breach of information occurs by the actions of their employee.

IF INSURANCE BOND IS NOT PROVIDED BY THE OUTSIDE BUSINESS SERVICE FOR THE ASSIGNED EMPLOYEE TO THE COMMUNICATIONS DIRECTOR/CHIEF, NO ACCESS TO COMPUTERS, NETWORKS, OR SOFTWARE SHALL BE ALLOWED.

Section 5: Asset Management

5.1 Information Classification

The District information, whether in electronic or physical form, can be categorized into three classifications. Due care must be taken to protect the District information assets in accordance with the three classifications, as described within this policy.

1. Confidential – Sensitive personally identifiable information (PII) used for business or educational purposes within the district which, if disclosed through unauthorized means, could adversely affect the district personnel, including employees and constituents, and could have legal, statutory, or regulatory repercussions. Examples include: information exempt from disclosure under the Freedom of Information Act (FOIA), information protected from disclosure under the Federal Health Insurance Portability and Accountability Act (HIPAA), criminal information pertaining to NCIC and CJIS, other personnel information including Social Security numbers, and personal financial information including Information Security Policy credit card data protected by the Payment Card Industry‘s Digital Security Standard (PCIDSS).

2. Internal – Information related to the school district business and educational information that if disclosed, accessed, modified or destroyed by unauthorized means, could have limited or significant financial or operational impact on the district. Examples include: strategic plans, vendor’s proprietary information, and responses to Requests for Proposals (RFPs), information protected by intergovernmental non-disclosure agreements or other non-disclosure agreements, and design documents. Other information related to the districts information technology that is considered Internal includes Firewall configurations, system designs and access point Internet Protocol (IP) addresses.

3. Public – Information intended for unrestricted public disclosure in the course of the school district’s business. Examples include: press releases, public marketing materials, and employment advertisements, school notices

Section 6: Responsibility for Assets

6.1. Ownership of Assets

All information stored and processed over the school district technology systems is the property of the North Providence School District. Users of the system have no expectation of privacy associated with the information they store in or send through these systems, within the limits of the federal, state, and local laws of the United States and, where applicable, foreign laws.

6.2. Acceptable and Unacceptable Use of Assets

6.2.1 To effectively conduct school district business and operations, the District makes available to authorized employees and third parties' various information technology resources, including e-mail, the Intranet, the Internet, and other communication and productivity tools. Use of these resources is intended for business or educational purposes in accordance with user's job functions and responsibilities, with limited personal use permitted only in accordance with a school district's personnel rules, this policy, and other applicable school district policies. The limited personal use of information technology resources is not permissible if it creates a non-negligible expense to the District, consumes excessive time, or violates a District policy or independent school policy. The privilege of limited personal use may be revoked or limited at any time by the communications director or school department officials.

6.2.2 Users must not allow any consultant, visitor, friend, family member, customer, vendor, other school district employee or other unauthorized person to use their network account, e-mail address, or other District provided computer facilities. Users are responsible for the activities performed by and associated with the accounts assigned to them by the District.

6.2.3 No user may use school district-provided Internet or Intranet access or the District's Confidential or internal information to solicit or conduct any personal commercial activity or for personal gain or profit or non-district approved solicitation.

6.2.4 Users must not make statements on behalf of the District or disclose confidential or internal District information unless expressly authorized in writing by their department head. This includes Internet postings, bulletin boards, news groups, chat rooms, or instant messaging.

6.2.5 Users must protect confidential or internal information being transmitted across the Internet or public networks in a manner that ensures its confidentiality and integrity between a sender and a recipient. Confidential information such as Social Security numbers, credit card numbers, and electronic Protected Health Information (ePHI) must be transmitted using encryption software. (Password protected documents or spread sheets)

6.2.6 Internal information such as email lists, must not be posted to any external information source, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the prior express written permission of the user's Department Head or Principal.

6.2.7 Users must not install software on the District network and computer resources without prior express written permission from the Director of Communications. Person-to-person (P2P) applications, Voice over IP (VOIP), instant messenger (IM) applications, and remote access applications pose an especially high risk to the District and their unauthorized use is strictly prohibited. School district business must not be conducted on any device that allows P2P communication (such as file sharing music applications or programs like Dropbox's) without explicit approval from the Director of Communications.

6.2.8 Users must not copy, alter, modify, disassemble, or reverse engineer the districts authorized software or other intellectual property in violation of licenses provided to or by the district. Additionally, users must not download, upload, or share files in violation of U.S. patent, trademark, or copyright laws. Intellectual property that is created for the district by its employees, vendors, consultants and others is property of the District unless otherwise agreed upon by means of third party agreements or contracts.

6.2.9 Users who store documents and or spreadsheets containing any personal or financial account information in shared folders for use between different District departments or schools shall encrypt those documents with a password.

6.2.10 Users must not access the Internet, the Intranet, or e-mail to use, upload, post, mail, display, or otherwise transmit in any manner any content, communication, or information that, among other inappropriate uses:

a. ***interferes with official North Providence School District business;***

b. ***is hateful, harassing, threatening, libelous or defamatory, pornographic, profane, or sexually explicit;***

c. ***is deemed by the District to offend persons based on race, ethnic heritage, national origin, sex, sexual orientation, age, physical or mental illness or disability, marital status, employment status, housing status, religion, or other characteristics that may be protected by applicable civil rights laws;***

d. ***impersonates a person (living or dead), organization, business, or other entity;***

e. ***enables or constitutes gaming, wagering, or gambling of any kind;***

f. ***promotes or participates in unauthorized fundraisers;***

g. ***promotes or participates in partisan political activities;***

h. ***promotes or participates in unauthorized advertising of District projects and any advertising of private projects;***

i. ***compromises or degrades the performance, security, or integrity of the District technology resources and information assets;***

j. ***contains a virus, logic bomb, or malicious code;***

k. ***Constitutes participation in chain letters, unauthorized chat rooms, unauthorized instant messaging, spamming, or any unauthorized auto-response program or service.***

l. ***Users may not transmit emails with any information in the above section B-2 unless done so from an authorized email address account issued by the Communications Department. The use of personal email accounts or ones created by anyone shall never be used to transmit district information. This included any and all correspondences between administrators, teachers, staff members, students, and parents.***

m. ***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.***

n. ***Use of Drop Box, Sky Drive or any similar site for the transfer of files is prohibited unless authorized by the Director of Communications.***

SECTION 7: Human Resources Security

7.1 <u>Prior to Employment</u>

All employees, consultants, and contractors who use the District information technology as part of their job function are required to sign the North Providence School District Computer Use Policy. Furthermore, employees must sign and accept individual school district department policies, rules and regulations, or standard operating procedures that pertain directly to a department’s individual uses of the District technology and its infrastructure. At no time shall a school or administrative office individual policy contradict a district policy were it lowers the requirements of the district security. In the event that a local school or administrative office policy is found to be written that contradicts the District security policy or increases the risk of threat to the District networks, the North Providence School District policy will supersede any local school or administrative office policy.

Consultants and contractors who are hired to support the District information technology Infrastructure must be able to provide proof of background checks (including a statement of what checks are conducted and how they are conducted) prior to accessing the districts information technology infrastructure. The background checks must include a criminal background check and or any other checks required by RIDE if physical access inside schools are needed to support the North Providence School District network.

7.2 During Employment

7.2.1 Information Security Awareness, Education, and Training

Security Awareness begins during the hiring process and it is the responsibility of the user to remain aware of current security policies. The School District Web-site contains the Districs Information Security Policy and Computer Use Policy.

Users should read the Security Reminders that are periodically distributed by email.

7.3 Disciplinary Process

Any violation of this policy, or any part or provision hereof, may result in disciplinary action, including termination and/or civil action and/or criminal prosecution. Any disciplinary action will be handled by the District Human Resources Director and will follow all appropriate contractual agreements. The User is also subject to any local school or administration department SOP's, rules, or regulations that describe disciplinary actions.

7.4 Termination or Change of Employment

7.4.1. Return of Assets

When a User leaves the district, all Information Assets remain the property of the North Providence School District. A user must not take away such information or take away a copy of such information when he or she leaves the District without the prior express written permission of the District.

7.4.2. Removal of Access Rights

Upon termination of an employee or vendor, the person who requested access to technology resources must request the termination of that by contacting the Communications Director in the event that the requestor is not available, the responsibility is placed upon the Administrative Office Department Head or Principal. The Director of Communications may automatically disable or delete accounts where termination is suspected even if formal notification was by-passed.

SECTION 8: Communications and Operations Management

8.1. Protection against Malicious Code

8.1.1 It is the North Providence School District policy to conduct virus scanning of its technology resources to protect them from the threat of malicious code. Though not all viruses or malware can be prevented from accessing the networks or its computers the District will try to intercept and/or quarantine any networking and computer resource that poses a virus threat to its information assets.

8.1.2 All servers and workstations (networked and standalone) must have the District approved antivirus protection software installed, properly configured, and functioning at all times.

Additionally, systems that have not been issued by the District but that are allowed to use the District network must also be protected by antivirus software. This includes but not limited to teachers and staff, personal laptops, iPad, tablets, smartphones.

8.1.3 All incoming and outgoing e-mails must be scanned for viruses.

8.1.4 Users are responsible for ensuring that files and data downloaded onto the districts workstations are that of school departments business only.

8.1.5 Users must NOT install any software on a district/school owned computer. Any required media devices must not be connected without first contacting the Department of Communications to check and insure that they are safe to the district's network.

8.1.6 The District must ensure that all workstations (networked and standalone) have the most current antivirus signature files loaded.

8.2 Back-Up

8.2.1 The District will perform regular backups of User files stored on the district file servers and storage media that are centrally managed by the Communications Department. Any other backup process will be coordinated in conjunction with the Districts user departments based on their individual business or educational needs.

8.2.2 The District will not back up any personal multimedia files in formats including, but not limited to, .mp3, m4a, m4p .avi and .mov. Any of this data found on the District network will be deleted without any notification to the user.

8.2.3 Requests for recovery of data shall be made to the Communications Department. At no time shall a file be recovered unless it was created or in use be the requester or by the Superintendent or designee.

8.2.3 System backups are conducted on a nightly bases and completion of backups are reported to the IT staff via email notifications. In the event a backup has failed the Communications Department shall research the problem and make needed corrections as soon as possible. Once corrected the backup should resume. There shall be 6 daily backups saved on storage media. Previous backup data will be written over upon completion of day 6.

8.2.4 Any backup data is stored in the Data Center or Data Substation location within town property. Those locations are subject to a separate Policy titled "Data Center site Security Policy"

8.2.5 A backup of data will be conducted on any application that is upgrading or converting data from one program to another or from one system to another.

8.3 Media Handling

9.3.1 Disposal of Media

a. Except as otherwise provided by law or court order, electronic information maintained in an administrative department ‘s office or school in the form of disks, portable drives, or usb media devices will be destroyed by department staff or Communications Department when the retention period expires or when no longer needed and those devices must be physically destroyed. Disks must be shredded; portable drive must be completely formatted. If any department is unable to complete the required process to dispose of a media device according to procedure they must contact the Communications Department to do so for them.

b. Any computer, printer, copier, fax machine, or other devices that stores media that has been used by the District that was on loan, lease agreement or is at end of life and will be decommissioned shall have its hard drive removed and destroyed by the Communications Department prior to it leaving district property. No vendor shall be allowed to take any device without the express permission from the Communications Director.

8.4 Monitoring

9.4.1 Monitoring System Use

a. Users should have no expectation of privacy in their use of Internet services provided by the district. The district reserves the right to monitor for unauthorized activity the information sent, received, processed or stored on district-provided network and computer resources including wi-fi, without the consent of the creator(s) or recipient(s). This includes use of the Internet as well as the Districts e-mail and any instant messaging systems; google drives; google classrooms. .

b. All information technology system administrators, technicians and any other employees who by the nature of their assignments have privileged access to networks or computer systems will be allowed to do so under the approval of the Director of Communications. Administrative Office Department Heads and Principals will be notified as to who has access to programs they manage. Administrative Office personnel and Department Heads understand that granted access is given to those staff members until the access is denied by the Director of

Communications. Access to systems are subject to any departments unique requirements such as federal, state, or department required certifications, background checks, or tutorials.

8.5 Clock Synchronization

All server clocks must be synchronized in a manner approved by the Director of Communications in order to provide for timely administration and accurate auditing of systems.

SECTION 9: Access Control

9.1. User Access Management

10.1.1 User Account Management

a. Access to Confidential and Internal data must be made to the Communications Director in a written request.

b. User accounts that have not been used for 90 days may be disabled without warning.

c. Administrative Office Departments must notify the Director of Communications of a change in employment status (such as when a User takes a leave of absence, transfers schools, or is terminated). The account of a User on a leave of absence can be retained, suspended, or deleted at the discretion of the Superintendent of the district. Accounts may include district issued e-mail addresses.

10.2.2 Access to applications

a. Application access is governed by each Administrative Office Department Head or Principal who manages the software program. Access is granted to those users either directly by the Department Head or by the Communication Department at the direction of the Administrative Office Department Head or Principal.

b. At no time shall an Administrative Office Department Head or Principal allow non Administrative Office Department Head or Principal users access to assign users rights.

c. Access rights to applications and programs that are shared by Administrative Office Departments or schools but are not owned by a specific department shall be given by the Communications Department after written consent by an Administrative Office Department Head or Principal.

d. For the purpose of clarification the Town Finance Control is deemed responsible for the Munis Financial application.

e. Access to applications data via interfaces being software or hardware based shall not be connected to any district or town database unless it is approved by the Communications

Director. Also each application developers must insure by means of approval or certification that its software will not cause functionality problems with each other.

f. Local admin rights to desktop computers shall not be allowed unless it stops users from accessing programs associated with the State or Federal applications. Allowing this controls considerably reduces the security of districts data and puts the district at a higher risk for intrusion and acceptance of malware. The Communications Department is completely against giving these local admin rights to any user. However due to programs that are used by the Federal or State Government some will not work without these rights. The Administrative Office Department Head must approve the installation of these programs and understand of their implications to the network and computers and accept the risk of computers being infected and understand the possible effects it will have on user production during computer down time for repairs. NO PROGRAMS WILL BE ALLOWED ON A DISTRICT COMPUTER OR NETWORK THAT REQUIRES LOCAL ADMIN RIGHTS.

Exception: The Director of Communications may at his or her discretion all Tech Lab teacher's local admin access only to desktop computer within a school lab only if he/she feels that Tech Teacher has the clear understanding of the risks involved and the confidence in that teacher's ability to perform the tasked needed on those computers without jeopardizing and security or operation of those computers.

9.2. <u>User Responsibilities</u>

10.2.1 Password Use

a. All e-mail, network, domain accounts must be password protected. All new e-mail accounts will be created with a temporary password. The temporary password must be changed upon first use.

b. District owned and issued mobile devices must be password protected; this includes but is not limited to personal digital assistants (PDA), smart phones, laptops, handhelds (e.g. Blackberries) and off-site desktops.

c. Passwords used on the district systems and on non-district systems that are authorized for use must have the following characteristics unless otherwise approved by the Director of Communications:

i. Passwords must be a minimum of 8 characters in length;

ii. Passwords must contain both alphabetic and numeric characters;

iii. Passwords must not be the same as the username;

iv. Passwords must not contain proper names or words taken from a dictionary;

v. Passwords must be changed at the direction of the Communications Director.

vi. Passwords used for production systems must not be the same as those used for corresponding non-production system such as the password used during training.

d. Passwords must not be disclosed to anyone. All passwords are to be treated as confidential information.

e. User ID's may not be shared with other persons.

f. Authorized users of the District's technology systems shall not share or use anyone else's password. Attempting to do so is prohibited. The creation of additional unauthorized passwords is prohibited. EXCEPTION: Authorized user shall share their password with a known Communications Department / IT Department staff member for troubleshooting or hardware/software installation or deletion purposes.

g. It remains the responsibility of each assigned user to safeguard their passwords to prevent unauthorized access. Users are not to visually display their passwords at or in close proximity to their workstations such as under keyboard, telephone, or mouse pad. Furthermore, the storage of passwords in an unlocked office or classroom door visual when open shall not be allowed.

h. Any vendor requiring access to a computer or server for a project that has been approved by the Communications Director shall be granted a username and password that will automatically expire within 15 days. That account will allow access only to the specific locations as to what is needed for the project. Access to folders or document will not be allowed unless approved by the Administrative Office Department Head. If a project is expected to extend longer than 15 days, the account may be granted and extension by the Director. If an extension is granted it shall be the Administrative Office Department Heads responsibility to notify the Communications Director that the project is complete and the vendor no longer need access to the account. If while conducting audits, reviews, or work on a sever Active Directory an IT staff member finds any vendor accounts that are still active for more than 30days shall contact the Administrative Office Department Head for that vendor and check its status. If the Department Head cannot be contacted at that time the Technician shall disable to account immediately and notify the Director of Communications to follow up with the Department Head.

9.3. Screen Savers

Use of password-protected screen savers is recommended to prohibit unauthorized system access. Screen savers should initiate after 20 minutes of inactivity. Password-protected screen savers are required on workstations that access confidential information such as electronic Protected Health Information. Password-protected screen savers are also required on workstations that access internal information if the workstation is not in an area that has restricted access.

Users must ensure that system access is locked or logged-off when they are away from their workstation.

9.4. Mobile Computing and Remote Access

9.4.1 Laptops, off-site computers, and cell phones, that contain confidential information (such as dept e-mails) must be password protected for access each time the device is handled. Protection methods such as a 4-digit numerical password or a drawing pattern may be used. Drawing patterns must have at least a pattern of 4 line points. Mobile media that contain internal information must be protected using an encryption technique approved by the Director of Communications, a strong logon password, or restricted physical access in order to protect the data. Examples of mobile media include flash drives, DVDs, CDs, and external hard drives.

9.4.2 Personal media devices (for example, MP3 players such as iPods) must not be used as peripheral devices on district-issued workstations.

9.4.3 Remote access is not possible by the District networks but can be provided by the town-network as an information conduit to assist in the accomplishment of municipal duties and goals at the discretion of the Director of Communications. Any other use is strictly prohibited. Requests for remote access must have a valid business reason and be approved by the Director of Communications. Due to the existing system infrastructure and limited amount of Remote access availability the Director of Communications must review the request for remote access and it shall be granted on an absolute necessity. Also anyone that has remote access may be at any time removed from that access if the Director feels there is another request of more priority if VPN tunnels are not available.

9.4.4 All remote access connections must be through a secure, centrally administered point of entry approved by the Town. Authorized remote access connections must be properly configured and secured according to Town-approved standards including the town’s password policy. All remote desktop protocol implementations must be authorized by the Director of Communications. Remote access through unapproved entry points will be terminated when discovered.

9.4.5 Non-district owned computer equipment shall NOT be used for remote access.

9.4.6 District owned computer used for remote access may at any time be requested to be returned to the district for inspections by the Communications Department.

9.4.7 Users with access to district email accounts such as but not limited to teachers, teacher’s aids, substitute teachers, counselors, therapists, psychiatrists who access their email outside of the District networks shall also have a passcode on their mobile

9.4.8 Any loss or theft of a mobile network device that has access to a District application or email account shall be reported to the Communications Director at time of recognition. Once notified all the users application accounts and network access will have a change in password required.

SECTION 10: Information Security Incident Management

10.1 Reporting Information Security Events and Weaknesses

10.1.1 Violations of the District Information Security Policy or any or all parts or provisions of this Policy must be reported to an Administrative Office Department Head, Principal, or to the Director of Communications. Any Administrative Office Department Head or Principal receives a complaint about the violation of this policy must try to validate its validity and if they feel it has violated the policy they must report it to the Communications Director. The Communications Director will also check its validity and if found to be in violation he/she must report it to the Human Resource Department and Superintendent for disciplinary action.

10.1.2 Users must ensure that the Communications Director is notified immediately whenever they feel a security incident occurs. Examples of security incidents include a virus outbreak, defacement of a website, interception of email, blocking of firewall ports, and theft of physical files or documents.

10.1.3 All reports of alleged violations of this policy, or any part or provision hereof, will be investigated by the appropriate authority. During the course of an investigation, access privileges may be suspended.

SECTION 11: Access/rights to folders

Administrative Office drive folders that reside on the District network are created by the Communications Department. Then in each department folder are department shared folders as well as individual user folders. Each department head and his or her designee have access to the entire department folder, then by approval of the department head access is granted to each user folder within that department folder. Anytime personnel are moved from one school/department to another the Communications Department shall be notified to move that individual’s folder to the new school/department folder and proper rights given for access.

11.4 OTHER DISTRICT COMPUTERS ON LOCAL WORKGROUPS

Access to computers that are on local workgroups and not on networks will be setup the same way as the district network. The local disc folders will have a shared folder with rights granted by the principal/department head, and then the principal/department head will have access to each local user folder.

SECTION 12: Compliance

12.1 Compliance with Legal Requirements

13.1.2. Intellectual Property Rights

a. Intellectual Property that is created for the District by its employees is property of the North Providence School District unless otherwise agreed upon by means of third party agreements or contracts.

b. No user may transmit to, or disseminate from, the Internet any material that is protected by copyright, patent, trademark, service mark, or trade secret, unless such disclosure is properly authorized and bears the appropriate notations.

12.2 <u>Prevention of Misuse of Information Processing Facilities</u>

Users are prohibited from using the District processing facilities—including data center, network cabinets or closets, and other facilities housing the districts technology equipment—in any way that violates this policy, and federal, state, or municipal law, including, but not limited to, the District and Personnel Rules.

12.3 <u>Compliance with Relevant Laws and Regulations</u>

By virtue of the District's services to its students and their parents or guardians and the nature of its legal status, the district is covered by certain laws and regulations dealing with security and privacy of information, most notably the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry 's Digital Security Standard (PCI DSS). These laws and regulations, in some circumstances, may require additional safeguards for protection the District's information beyond the stipulations of this policy. (For example, when accessing credit/debit cardholder data remotely for the purposes of the school lunch program, it is never to be stored on local hard drives, floppy disks, or external media. Furthermore, cut-and-paste and print functions are prohibited during remote access sessions.) Accordingly, users with access to Protected Health Information (PHI) must abide by HIPAA and users with access to credit/debit card information must abide by PCI, as applicable.

12.4 <u>Compliance with Security Policies and Standards</u>

All Users must read and sign the District Computer Use Policy and the North Providence School Information Security Policy prior to being authorized to access the District information technology and information assets. *(Any user currently using the districts information technology and information assets prior to 2020 that has not already signed the updated policy shall signed the updated policy before the end of the first month approved by school committee or access will be suspended).*

SECTION 13: Reviewing and updating of Policies

13.1 The Communications Department on an annual basis will conduct a review of the District network infrastructure and update its policies and SOP's if needed. In the event a security issue arises the Communications Department will immediately take action and protect its assets and will make notification to its users of proper handling of potential threats and reminders will be sent to users on how to handle receiving unknown emails or emails with attachments.

13.1.2 The Communications Department will include its Director, Systems administrator, Network Manager, and Technicians as a team to review its infrastructure and venerability.

SECTION 14: Violations/Disciplinary actions

14.1 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 Collective Bargaining Agreement.

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.

SECTION 15: Incident Response and Data Breach Notification procedure

This ***Incident Response and Data Breach Notification Plan*** ("the Plan") is intended to provide a well-defined, organized approach for handling any potential security breaches, or threats to the North Providence's School District network data. The Plan defines what constitutes a security incident, identifies areas of responsibility, and establishes documentation and assessment procedures. This Plan has the following objectives:

- Identify an Incident Response Team –Provide information about the personnel who will be involved in the incident response and define their roles and responsibilities.
- Detail our Incident Response – Define the actions to be taken when an incident occurs.
- Prevention – Improve processes and procedures to help prevent the security incident or breach from reoccurring.
- Restoration –Present an orderly course of action for restoring functionality after an incident.
- Documentation – Collect and document as much information about the incident as possible.
- Review – Review policies, procedures and technology, and update as necessary.
- Mitigation –Implement processes to mitigate the effects of the security incident or data breach.

The Communications Department strives to prevent breaches of personal information ("PI") electronically or otherwise and maintain privacy and security measures to protect the confidentiality of PI. "PI" is defined by applicable state law(s). The Communications Department has implemented reasonable and appropriate safeguards to protect the confidentiality, security and privacy of PI in its possession.

II. Scope

The Plan applies to all School District employees. All employees are expected to follow the procedures set forth below and report any suspected and/or confirmed breaches of security to the building administrator and the Director of Communications or his/her assistant.

III. Incident Response Team

An Incident Response Team will be established to provide a quick, effective, and orderly response to suspected and/or confirmed data breaches and security incidents. The Incident Response Team will be authorized to take appropriate steps deemed necessary to contain, mitigate or resolve a security incident. The Incident Response Team will consist of the following members:

- ✓ Director/Chief of Communications and Technology
- ✓ Assistant Technology Director
- ✓ System Administrator
- ✓ Superintendent of Schools
- ✓ Assistant Superintendent of Schools
- ✓ School Finance Director
- ✓ School Human Resource Director
- ✓ School Attorney

Other outside legal counsel may also be a member of the Incident Response Team.

The personnel and/or department participation on this team may change based upon the priority and scope of any given security incident as determined by the then current Incident Response Team.

The objectives of the Incident Response Team include the following:

- Incident handling and investigation;
- Coordination of responses to incidents;
- Communication with personnel;
- Notification to regulatory authorities;
- Coordination with third-party service providers;
- Liaison to law enforcement; and,
- Notification to individuals.

The Incident Response Team should also:

- Coordinate with incident response services of a third-party security firm and outside legal counsel as appropriate;
- Review information received from the individual(s) reporting the security incident or breach;
- Implement processes to prevent alteration to the system(s) until a backup has been completed;
- Implement processes to perform a full backup of the system(s) to forensically sterilize media (i.e. disk imaging) and store the backup in a secure area as an important part of the chain of custody (as applicable)
- Work with other departments and information technology staff, as appropriate, in determining the risk of continuing operations (e.g. deciding whether to shut down system, disconnect from network, continue operation, etc.); however, any decision to delay the containment should be discussed with legal counsel based on the liability;
- Implement processes to change passwords or other security safeguards on any compromised systems; and,
- Maintain detailed documentation on all actions taken.

IV. Procedure

If a system intrusion has occurred where data might have been compromised the Incident Response Team should:

- Determine where and how the intrusion occurred.
- Identify the source of compromise, and the timeframe involved.
- Determine if an intruder has exported or deleted any data.
- Review the network to identify all compromised or affected systems.
- Look at appropriate system and audit logs for each type of system affected.
- Document all internet protocol (IP) addresses, operating systems, domain system networks and other pertinent system information.
- Determine if the source was an employee, third party or vendor.
- Engage forensic analysis as necessary.

Once the incident has been contained, Director of Communications should communicate to the Incident Response Team the following information:

- The extent of the damage (if any) and the data potentially affected (if any);
- The current status of the incident;
- Which systems were affected;
- The expected time of resolution (if known).

V. Notification

Confirmed breaches of the security or privacy of PI will invoke certain actions to determine whether the PI has been compromised according to applicable state law(s), and whether, under those state law(s), notification of the breach will be made to the affected individual(s).

The Communications Department has implemented reasonable systems for the discovery and reporting of a breach of PI. Generally, for purposes of this procedure, a “breach” of PI is the unauthorized acquisition, access, use or disclosure, or reasonable belief of unauthorized acquisition, access, use, or disclosure, of PI that compromises the confidentiality, security or privacy of the PI. However, depending on the circumstances of the breach, the Incident Response Team, in conjunction with its outside legal counsel, will assess the applicable state law(s) to determine if a breach has occurred in accordance with the applicable statute(s).

When a breach has been reported, an investigation into the breach will be conducted.

- The investigation and steps taken will be thoroughly documented. If at the conclusion of the investigation it is determined that no breach occurred, no further action is necessary, but the investigation and conclusion will be thoroughly documented.
- If it is confirmed that a breach of security or confidentiality has occurred and has resulted in the unauthorized access, use or disclosure of PI, the Incident Response Team will conduct an investigation and an assessment of applicable state breach notification law(s). The investigation and assessment will be documented thoroughly, including the actions taken, the conclusions of the assessment and the basis for the determination that there was or was not a breach of PI in accordance with the applicable state law(s).
- If it is determined that the PI was breached, and notification is required, an analysis of the requirements for notification of the state(s) in which the individual(s) reside will be conducted and documented.
- If notification to law enforcement or another regulatory body or agency is required under state law(s), such notification will be made to the regulatory body or agency in accordance with state law(s).
- If state law(s) requires notification to the individual(s), notification will be made in accordance with state law(s). The notification will include any information required by applicable state law(s).

The Communications Department requires all third-party contractors and vendors to provide notification of a breach to The Communications Department so affected individuals can be notified, as necessary.

The School Finance Director will notify the district insurance carrier of the breach.

If necessary, the Incident Response Team will assemble a list of vendors to aid in the notification requiremen in accordance with state law(s):

✓ Outside legal counsel;

- ✓ Notification services;
- ✓ Credit monitoring/identity theft management/call center;
- ✓ Forensic investigation vendor;
- ✓ Crisis management.

VI. Prevention

After the incident has been stabilized and mitigated, the System Administrator should verify the exploit or system(s) affected are patched, hardened or reconfigured to prevent further exploits or infections from reoccurring. If the incident did not involve Communications Department electronic systems (i.e. a third-party vendor caused the breach/incident), the Incident Response Team should revise/implement appropriate processes and procedures to prevent a similar incident in the future.

VII. Restoration

After the prevention procedures are completed, the Systems administrator should work towards bringing the system(s) affected back to functional state. Care should be taken to preserve any evidence of an intruder by backing up logs or the entire system(s) affected. If the incident did not involve North Providences electronic systems, the Incident Response Team should utilize appropriate physical safeguards and/or take appropriate action related to the third-party's acts or omissions related to the incident.

VIII. Documentation

Systems Administrator

The Systems Administrator should collate all technical documentation (logs, system events, exploit descriptions and other information) regarding the incident, the effects of the incident and any damage incurred from the incident, preservation of all evidence and the steps taken to restore functionality. This documentation should be given to the Assistant Communications Director. The Assistant Communications Director should document any processes and procedures, and investigative notes, regarding all other security incidents not involving electronic data.

Director and Assistant Communications Director

The Director and Assistant Communications Director should prepare a written summary of the incident and corrective action taken steps taken to restore functionality. A copy of this documentation should be included with the documentation obtained during the final assessment of the incident. As applicable the technical documentation, data files and other literature from the Systems Administrator and shall maintain copies of all notifications sent to individual(s) and/or regulatory body and/or agency.

VIIII. Review

The members of the Incident Response Team should meet frequently during an incident and to review the complete details of the incident, review all technical documentation (logs, system events, exploit descriptions and other information) and the steps taken to restore functionality. Questions to be answered include:

- Assess damage and cost; assess the damage to School Districts infrastructure and estimate both the damage cost and the cost of the containment efforts.

- Review response and update policies, procedures and guidelines; plan and take preventative steps so the intrusion will not recur.
- Consider whether a procedure or policy was not followed which may have led to the intrusion,
- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed in a timely manner?
- Were the incident response procedures followed appropriately? How can they be improved?
- Are all systems patched, systems locked down, passwords changed, anti-virus updated, and appropriate procedures, guidelines and policies in place, etc.?
- Have changes been made to prevent a new and similar incident?
- Should any security policies be updated?
- What lessons have been learned from this experience?

The members of the Incident Response Team should determine what steps (if any) should be taken to help prevent against similar incidents from occurring. Security policies, procedures and/or guidelines may need to updated to include new threats as they arise. This Plan should be updated as necessary so appropriate response instructions to incidents can be achieved.

X. Responsibility

This procedure will be maintained by, and updated as necessary by, the Director of Communications

XI. Distribution of the Plan

The Plan will be available in printed form to all Incident Response Team members to securely maintain in their office and/or workstation. Copies of the Plan will be distributed to other employees as appropriate.

XII. Testing and Annual Maintenance

Review of the Plan and conducting of incident response exercises (i.e. tabletop scenarios) will be performed periodically, at least once annually.

Appendix A – Common Terms and Definitions

1. Computer Resources - All related peripherals, components, disk space, system memory and other items necessary to run computer systems.

2. Credit Card Data - The Primary Account Number (PAN), Card Verification Value (CVV--the 3-4 digit code on the signature block on the back of a Credit Card), track data (the data read directly from the magnetic stripe of a Credit Card) and PIN Block data (also read from the magnetic stripe). The PCI DSS can be found at https://www.pcisecuritystandards.org.

3. Department Management - A supervisor, manager, director, Superintendent, or other employee of the North Providence School District designated by the North Providence School Committee to be responsible for implementation of this Policy.

4. 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.

5. Information Assets - Information and data created, developed, processed, or stored by the district that has value to the districts business or educational purposes.

6. Information Technology or Network and Computer Resources - Computer hardware and software, network hardware and software, e-mail, voice mail, video conferencing, facsimile transmission, Digital and analog voice recordings, telephone, remote access services, printers, copiers, and all other printed and electronic media.

7. Intranet - The suite of browser-based applications and HTML pages that are available for use only with access to the districts internal network.

8. 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.

9. Internet Services – Any service in which its primary means of communication is the Internet. For example e-mail, web browsing and file transfers.

10. Mobile Computing Devices – Mobile devices and Mobile media. Mobile data processing devices are used as business and educational productivity tools. Examples include: laptops, personal digital assistants (PDAs), smart phones, handhelds (e.g. Blackberries), and off-site desktops. Mobile media are devices typically used to transport data. Examples include: flash drives, DVDs, CDs, and external hard drives.

11. Network - 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.

12. P2P – Peer-to-Peer network. A network where nodes simultaneously function as both ―clients‖ and ―servers‖ to other nodes on the network, P2P may be used for a variety of uses, but it is typically used to share files such as audio files.

Examples of P2P networks include Napster, KaZaA, and LimeWire, If a node is not properly configured, any file on the device may potentially be accessed by anyone on the network.

13. Protected Health Information – Individually identifiable health information about an individual that relates to the past, present, or future physical or mental health or condition, provision of health care, or payment for health care. The related to employees, students, parents or guardians.

14. Remote Access Services – A service that enables off-site access to the districts information technology and assets.

Examples include the districts telephone exchanges, internal phone switches, wireless access points (WAP), and Virtual Private Network (VPN) connections. Remote access includes, but is not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems.

15. Security Incident – An event that has an adverse impact on the confidentiality, integrity, and availability of computer systems, computer networks, electronic information assets, or physical information assets.

16. User(s) – The school departments committees, boards, administrative office employees, temporary employees, teachers, teacher assistances, student teacher, teacher aids, psychiatrists, therapists, councilors, custodians, students, interns, vendors, consultants, contractors, volunteers, PTA members, and authorized agents who utilize the North Providence School district information assets and technology.

17. World Wide Web (WWW) – Browser-based applications and HTML pages that are available for access and use across the Internet.

NORTH PROVIDENCE SCHOOL DISTRICT
INFORMATION SECURITY POLICY
USER AGREEMENT

By signing below, I hereby acknowledge that I have received and read a copy of the “North Providence School District Information Security 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 North Providence 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

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