IJNDB-R

EMPLOYEE USE OF NETWORK RESOURCE AND TELECOMMUNICATIONS (NRT) SYSTEMS

The Nashua School District has established this policy with regard to access and disclosure of information composed, stored, sent, or received by employees using the District's Network Resource and Telecommunications Systems (NRT). This policy shall apply regardless of the physical location of the employee when accessing the District's NRT systems.

- Employees of the District shall communicate in a professional manner consistent with City, State, and federal laws, rules and regulations, including, but not limited to, those governing the behavior of school employees and federal copyright laws.
- NRT systems are to be used for business purposes only, with the following exception: Personal use of NRT systems during working hours is permitted on a very limited basis as long as it does not interfere with the employee's job performance or the operations of the District, does not otherwise violate this policy or any other District policies, and does not result in additional costs to the District.
- NRT systems are owned by the District. All messages, data, or conversations (information) composed, stored, sent, or received using these systems, including erased files that are recoverable, are and remain the property of the District.
- All staff shall keep classified district data, outlined in the Data Governance Plan (Appendix E), within the Nashua School District environment. District emails and other data originating and sent to the @nashua.edu and @nsd42.net domains are considered classified at the highest levels, which include Personally Identifiable Information, Confidential Information, Internal Information, and Directory Information (Data Governance Plan, Appendix E). Under no circumstances shall data leave NRT systems by way any means including, but not limited to, email forwarding, physical media, photo, etc. The Information Security Officer, Deputy Information Security Officer, and Superintendent reserve the right to investigate any violations. This excludes Union-related business with employees' bargaining group.
- The District reserves, and may exercise without prior notice, the right to read, review, audit, intercept, access, or disclose any and all information composed, stored, sent, or received by employees over NRT systems for any purpose, even if coded or passworded. Notwithstanding the District's right to retrieve and monitor information as outlined herein, such information should be treated as confidential by other employees and accessed only by the intended recipient. Any exception to this policy must receive prior approval by the Superintendent.
- NRT systems may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.
- The District prohibits the sending of discriminatory, harassing, or offensive materials in any form of media. Among those which are considered offensive are any messages or pictures which contain sexual implications, racial slurs, gender-specific comments, or any other comments that offensively address someone's age, sexual orientation, religious or political beliefs, national origin, or disability. Use of the District's NRT systems is subject to the prohibitions contained in the Educators' Code of Conduct, Ed Administrative Rule 510.
- The District has the authority to terminate or limit access to any program or NRT system at any time.
- Violation of this policy may result in disciplinary action, up to and including, termination.

<u>District E-mail</u>

- In general, e-mail users are expected to communicate in a professional manner consistent with City, State, and federal laws, rules and regulations, including, but not limited to, those governing the behavior of school employees and federal copyright laws.

- Teachers and other staff members shall use e-mail only for educational and professional purposes, except as noted above.
- Communications over District e-mail accounts are not private. The District reserves the right to monitor traffic passing through its system. Ordinarily, this would be done only if the District suspects activities that do not comply with applicable laws or this policy.
- Use of e-mail for personal solicitation and benefit (for example, an e-mail sent out to staff advertising an apartment for rent) is strictly prohibited.
- Users should use extreme caution when communicating sensitive information using electronic mail.
- Access to District e-mail and all NRT systems will be terminated when an employee ends employment with the District.
- District employees shall take all necessary measures to maintain student privacy and protect student confidential information when using the District's NRT systems.

Procedures for the Use of District Loaned Laptop Computers

Laptop

Nashua School District provides laptop computers to faculty and staff members for school-related business. It is not intended as a replacement for, or use as, the employee's personal computer. Use of the laptop should be in compliance with the Nashua School District's published acceptable use policies (EHAA), and all applicable federal, state and local laws, rules and regulations.

Ownership of the Laptop

- Ownership of the laptop computer shall remain with the Nashua School District. Laptops and related equipment shall be returned when an individual's employment with the District terminates or sooner if requested to do so by the District.

Computer Configuration and Software Licensing

- The laptop will be configured with a standard suite of programs. It is possible that the content area or grade level supported will require unique programs. Users may make changes to the configuration of their laptop with permission of the IT Department. These changes may include installing software, adding printers or changing web browser setting.
- All applications used on the laptop shall be approved by the District's vetting process outlined in the District's Data Governance Plan in accordance of NH RSA: 189:66-68a.

Liability for Loss, Theft, or Damage

- It is the staff member's responsibility to take appropriate precautions to prevent damage to or loss/theft of the loaned laptop computer.
- The employees may be responsible for certain costs to repair or to replace the computer if the damage or loss is due to their negligence, intentional misconduct or noncompliance with these procedures.
- In case of theft or loss, the user shall:
    - Immediately report the loss to the user's school administration and the school's administration will notify the Department of Technology.
    - Assist the District in filing a report with the appropriate police department if the loss was the result of theft or other criminal behavior.

Security of Systems and Information

- Attempts to alter system software, to bypass security protocols, to introduce viruses, worms, or other malicious or destructive programs, or otherwise "hack" are expressly prohibited.

- All confidential data must be stored on all District network and locally secured drives, that include, but not limited to, District network servers, drives, and/or cloud storage (the "Z" drive, O365 One Drive, and Google Drive) consistent with Policy EHAA and other relevant laws, rules, regulations and policies. Users shall not store confidential data on their computers. Confidential data includes personal identifiable information (PII) of the user or other employees or students and any information that may compromise the personal safety of students or employees (See Data Governance Plan). If users choose not to store non-PII data on the network drives, they shall be responsible for maintaining appropriate backups. In the event of data loss due to the negligence or intentional conduct of the employee, the employee may be liable for the cost of service, hardware, or equipment for retrieval.

Support and Service

- In general, District support will only be provided to machines when the employee is on campus.
- Users experiencing technical problems should contact the help desk through the Department of IT at helpdesk@nashua.edu. As a result of repair and restoration, your serviced device may be restored to the District's original standard configuration. If a user has modified their laptop configuration, either by installing additional software or making other changes, it is the responsibility of the user to reinstall said software and/or to reconfigure the laptop.
- The Department of Technology will provide the services required to maintain or repair laptops should operation be impaired by a component failure or normal wear and tear.
- The Technology Department will neither provide Internet access to the user from off campus nor will be diagnosing any current home network. The Department of Technology will configure the device in a way that networks outside of the Nashua School District will be made visible and have the ability to connect to WIFI.

Legal Reference:

RSA 194:3-d, School District Computer Networks

Legal References Disclaimer*: These references are not intended to be considered part of this policy, nor should they be taken as a comprehensive statement of the legal basis for the Board to enact this policy, nor as a complete recitation of related legal authority. Instead, they are provided as additional resources for those interested in the subject matter of the policy.*

Board Approved: 10/16/2006
04/09/2007 (*Replaces POPPS 11500)*
12/21/2020
02/19/2024