

**DATA MANAGEMENT**  
(Public Use of School Records)

The Superintendent is hereby designated the custodian of all records, minutes, documents, writings, letters, memoranda, or other written, typed, copied, or developed materials possessed, assembled, or maintained by this District.

1. All requests for public information are to be forwarded to the Superintendent immediately upon receipt. The Superintendent shall thereupon make a determination as to whether or not the information requested is public in nature. If public, the Superintendent shall provide the information in a timely manner, which does not disrupt the operation of the schools.
2. In accordance with RSA 91-A:4, if the Superintendent finds the information to be public in nature, he or she shall direct that it be reproduced on the premises. The party requesting the information is to be charged the cost of reproduction and any other expenses entailed in locating and retrieving the information. If the information is in active use or otherwise unavailable, the party requesting the information will be notified immediately upon its becoming available.
3. If the Superintendent finds the information not to be public in nature, he or she shall so inform the requesting party and shall for no reason release such information.
4. If the Superintendent is unable to ascertain whether or not the information requested is public in nature, he or she is hereby authorized to request, on behalf of the Board, an opinion from the Board's attorney as to the nature of the information. Such opinion requests will be made within ten (10) days of the original request for the information. The Superintendent shall notify the person requesting such information that an opinion is to be requested of the attorney and shall notify such person immediately upon receipt of an answer from the attorney.

Statutory Reference:

RSA 91-A:4

Revised: July, 1998  
Revised: November, 1999  
Reviewed: June 9, 2003  
Reviewed: October 12, 2010

## SCHOOL ADMINISTRATIVE UNIT #79

EHAA

### COMPUTER SECURITY, E-MAIL AND INTERNET COMMUNICATIONS POLICY

The District has established this policy with regard to access and disclosure of electronic data composed, stored, sent, or received by employees using the District computer system. This policy is designed to protect the safety and security of the District's computer systems including E-mail and Internet use.

The District intends to enforce the rules set forth below and reserves the right to change these rules at any time.

1. The computer hardware system, software and E-mail system are owned by the District, and all messages or data composed, stored, sent, or received using the system are and remain the private property of the District. They are not the property of the employee.
2. The computer and E-mail system is to be used for business purposes only. Personal business is unauthorized and should not be conducted on the system.
3. The electronic mail system may not be used to solicit or proselytize for commercial ventures, religious or political causes, outside organizations, or other non-job-related solicitations.
4. The District prohibits discriminatory, harassing, or offensive materials in any form of media. Among those which are considered offensive are any messages 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.
5. The electronic mail system shall not be used to send (upload) or receive (download) copyrighted materials, trade secrets, proprietary financial information, or similar materials without prior authorization.
6. The District reserves, and intends to exercise without prior notice, the right to read, review, audit, intercept, access or disclose any and all information on an employee's computer system or messages created, received or sent over the electronic mail system for any purpose, even if coded or passworded.

**COMPUTER SECURITY, E-MAIL AND  
INTERNET COMMUNICATIONS POLICY (CONT'D)**

7. The confidentiality of any message or data should not be assumed. Even when a message is erased, it is still possible to retrieve and read that message. The use of passwords for security does not guarantee confidentiality, or that the District will not retrieve it. All passwords must be disclosed to the computer administrator.
8. Any communications created, sent, or retrieved using E-mail may be read by individuals other than the intended recipient.
9. Notwithstanding the District's right to retrieve and monitor any E-mail messages, such messages should be treated as confidential by other employees and accessed only by the intended recipient. Employees are not authorized to retrieve or read any E-mail that is not sent to them. Any exception to this policy must receive prior approval by the Superintendent.
10. Any employee who violates this policy or uses the computer system or electronic mail system for improper purposes shall be subject to discipline up to and including discharge.
11. The District has the authority to terminate or limit access to any program at any time.
12. Personal disks cannot be used on the system unless pre-authorized by the computer administrator.

Statutory Reference:

RSA 194:3-d

Revised: July, 1998  
Revised: November, 1999  
Reviewed: June 9, 2003  
Reviewed: October 12, 2010

## SCHOOL ADMINISTRATIVE UNIT 79

EHB

### DATA/RECORDS RETENTION

The Superintendent shall develop procedures for a records retention system that is in compliance with RSA 189:29-a and Department of Education regulations. The procedures should ensure that all pertinent records are stored safely and are stored for such durations as are required by law. Additionally, the Superintendent shall develop procedures necessary to protect individual rights and preserve confidential information.

*Legal References:*

*RSA 91-A, Right to Know Law*

*RSA 189:29-a, Records Retention and Disposition*

*NH Code of Administrative Rules, Section Ed 306.04 (a) (4), Records Retention*

*NH Code of Administrative Rules, Section Ed 306.04 (h), Records Retention*

*20 U.S.C.: 1232g. Family Educational Rights and Privacy Act (FERPA)*

Adopted: November, 1999

Reviewed: June 9, 2003

Revised: October 8, 2008