EMPLOYEE COMPUTER AND INTERNET USE RULES

NEPN/NSBA Code: GCSA-R

These rules accompany Board policy GCSA (Employee Computer and Internet Use). Each employee is responsible for his/her actions and activities involving school unit computers, networks and Internet services, and for his/her computer files, passwords and accounts. These rules provide general guidance concerning the use of the school unit's computers and examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity by employees. Employees who have questions about whether a particular activity or use is prohibited are encouraged to contact the Principal or the Technology Coordinator.

1. **Consequences for Violation of Computer Use Policy and Rules**
   Failure to comply with Board policy GCSA; failure to report a breach of computer security to the Principal or Technology Coordinator; or failure to comply with other procedures or rules governing computer use may result in disciplinary action, up to and including termination. Illegal use of the school unit's computers will also result in referral to law enforcement.
2. **Access to School Computers, Networks and Internet Services.**
   The level of employee access to school unit computers, networks and Internet services is based upon specific job requirements and needs. Unauthorized access to secure areas of the school unit's computers and networks is strictly prohibited.
3. **Acceptable Use**
   Rangeley Lakes Regional School's computers, networks and Internet services are provided to employees for administrative, educational, communication and research purposes consistent with the school unit's educational mission, curriculum and instructional goals. All Board policies, school rules and expectations for professional conduct and communications apply when employees are using the school unit's computers, networks and Internet services whether in use at school or off school premises.

D. **Personal Use**
School unit computers, network, and Internet services are provided for purposes related to school programs and operations, and performance of their job responsibilities. Incidental personal use of school computers is permitted as long as such use: 1) does not interfere with the employee's job performance; 2) does not interfere with system operations or other system users; and 3) does not violate this policy and the accompanying rules, and any other Board policy, procedures, or school rules. "Incidental personal use" is defined as use by an individual employee for occasional personal communications which do not interfere or conflict with his/her job responsibilities.

E. **Prohibited Uses**
Examples of unacceptable uses, which are expressly prohibited, include, but are not limited to, the following:

1. Any use that is illegal or which violates other Board policies, procedures, or school rules, including harassing, discriminatory, or threatening communications and behaviors; violations of copyright laws, etc. The school unit assumes no responsibility for illegal activities of employees while using school computers,

2. Any use involving materials that are obscene, pornographic, sexually explicit, or sexually suggestive, harmful to minors or intended to appeal to prurient interests

3. Any inappropriate communications with students or minors for non-school related purposes 4. Any use for private financial gain, or commercial, advertising, or solicitation purposes.

5. Any use as a forum for communicating by e-mail or any other medium with other school users or outside parties to solicit, proselytize, advocate, or communicate the views of an individual or non-school sponsored organization; to solicit membership in or support of any non-school sponsored organization; or to raise funds for any non-school sponsored purpose, whether profit or not-for-profit. No employee shall knowingly provide school Email addresses to outside parties whose intent is to communicate with school employees, students and/or their families for non-school purposes. Employees who are uncertain as to whether particular activities are acceptable should seek further guidance from the Principal or the Technology Coordinator.

6. Any communication that represents an employee's personal views as those of the school unit, or those that at could be misinterpreted as such.

7. Downloading or loading software or applications without permission from the Principal or Technology Coordinator. Unauthorized copying of software is illegal any may subject the copier to substantial civil and criminal penalties. The school unit assumes no responsibility for illegal software copying by employees.

8. Sending mass E-mails to school users or outside parties for school or non- school purposes without permission of the Principal or Technology Coordinator.

9. Any malicious use or disruption of the school unit's computers, networks, and Internet services; any breach of security features; or misuse of computer passwords or accounts (the employee's or those of other users).

10. Any misuse or damage to the school unit's computer equipment, including opening or forwarding E-mail attachments (executable files) from unknown sources and/or that may contain viruses;

11. Any attempt to access unauthorized sites, or any attempt to disable of circumvent the school unit's filtering/blocking technology/

12. Using school computers, networks and Internet services after such access has been denied or revoked; and

13. Any attempt to delete, erase or otherwise conceal any information stored on a school computer that violates these rules or other Board policies or school rules, or refusing to return computer equipment issued to the employee when requested.

F. **No Expectation of Privacy**
Rangeley Lakes Regional School's computers remain under the control, custody, and supervision of the school unit at all times. The school unit reserves the right to monitor all computer and Internet activity by employees and other system users whether on or off school premises.

Employees have no expectation of privacy in their use of school computers, including e-mail, stored files, and Internet access logs.

G**. Disclosure of Confidential Information**
Employees are expected to use appropriate judgment and caution in communications concerning

students and staff to ensure that personally identifiable information remains confidential. H. **Employee/Volunteer Responsibility to Supervise Student Computer Use**

Employees and volunteers who use school computers with students for instructional purposes have a duty of care to supervise such use. Teachers, staff members and volunteers are expected to be familiar with the school unit's policies and rules concerning student computer and Internet use and to enforce them. When, in the course of their duties, employees or volunteers become aware of a student violation, they are expected to stop the activity and inform the Principal or Technology Coordinator.

I. **Compensation for Losses, Costs and/or Damages**

The employee is responsible for compensating the school unit for any losses, cost, or damages incurred by the school unit for violations of Board policies and school rules while the employee is using school unit computers, including the cost of investigating such violations. The school unit assumes no responsibility for any unauthorized charges or costs incurred by an employee while using school unit computers.

J. **Any breach of computer security must be reported to the system administrator**.

Cross Reference: EGAD – Copyright Compliance;
EGAD-R – Copyright Compliance Administrative Procedure
GCSA - Employee Computer and Internet Use
GF – Staff Conduct With Students;
IJNDB – Student Computer Internet Use

Adopted: July 18, 2006
Revised: October 25, 2011
Revised: 12/12/2019; 2.6.2023