EMPLOYEE COMPUTER AND INTERNET USE RULES

These rules implement 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 a building administrator or the Technology Coordinator.

A. **Consequences for Violation of Computer Use Policy and Rules**

Failure to comply with Board policy GCSA, these rules, and/or 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.

B. **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.

C. **Acceptable Use**

School Department 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 communication apply when employees are using the school unit's computers, networks, and Internet services.

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 responsibilities and performance; 2) does not interfere with system operations or other system users; and 3) does not violate this policy and the accompanying rules, or any other Board policy, procedure, or school rules. "Incidental personal use" is defined as use by an individual employee for *occasional* personal communications.

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 behavior, 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;

3. Any inappropriate communications with students or minors;

4. Any use for private financial gain, or commercial, advertising, or solicitation purposes;

5. Any use as a forum for communicating by email 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 e-mail 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 building principal or other appropriate administrator.

6. Any communication that represents personal views as those of the school unit or that could be misinterpreted as such;

7. Downloading or loading software or applications without permission from the system administrator. Unauthorized copying of software is illegal and 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 emails to school users or outside parties for school or non-school purposes without the permission of the Technology Coordinator or building administrator.

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 email attachments (executable files) from unknown sources and/or that may contain viruses;

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

12.   Failing to report a breach of computer security to the system administrator;

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

14.   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 upon request.

F.   Employees and Social Media

Employees shall not accept or request current Lisbon students as friends on personal/professional social networking sites. This is not intended to prevent employees from friending a family member or close family friend, but employees are cautioned to consider these on-line relationships carefully. Employees of Lisbon School Department are mandated reporters to DHHS when, and if, they become aware of any potential abuse of student, whether at or away from work. Employees shall not post confidential information about students or staff.

The Lisbon School Department recognizes that the use of social media as a form of communication is becoming a preferred way for parents and students to communicate, however, staff shall redirect

parents and students to use your district email address for communication. We do recognize that staff may need to maintain school based social pages in an effort to provide mass information to groups they supervise.

G.   No Expectation of Privacy

School Department 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. Employees have no expectation of privacy in their use of school computers, including email messages and stored files, and Internet access logs.

H.   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.

I.   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 building principal.

J.   Compensation for Losses, Costs and/or Damages

The employee is responsible for compensating the school unit for any losses, costs, 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.

K. **Additional Rules for Laptops or Other Technological Devices Issued to Employees**

1. Employees are responsible for the proper care of laptops or other technological devices assigned to them at all times, whether on or off school property.

2. If a laptop or other technological device is lost or stolen, this must be reported to the building principal immediately.

3. The School Committee's policies and rules concerning technology and Internet use apply to the use of school department laptops and other technological devices at all times and places, on or off school property.

4. Laptops and other technological devices must be returned in acceptable working order at the end of the term of employment or whenever requested by a district administrator.

L. **Additional Rules for Laptops or Other Technological Devices Brought to School by Employees**

1. Before connecting to any Lisbon School Departments' network, an employee owned device must be checked for viruses and/or other compatibility by a representative of the technology office.

2. Any computer or other device that will be connected to a school department network must be free of viruses and must be running a current version of virus detection software. The devise must be configured in a way that is compatible with the school department policies and rules.

3. The School Committee's policies and rules concerning technology and Internet use apply to the use of personally-owned technological devices used on school grounds or during school activities.

4.   Violation of policies or rules governing the use of technology may result in the device being banded from use at school. The employee will also be subject to disciplinary action for any violations of School Committee policies or school rules.

5.   Lisbon School Department assumes no responsibility for the functioning or use of personally-owned technological devices on school grounds or at school activities.

Cross Reference: GCSA - Employee Computer and Internet Use

Adopted: March 13, 2000
Revised: January 8, 2007
Reviewed: March 08, 2010
Reviewed: March 11, 2013
Revised: May 11, 2015
Revised: April 11, 2016
Reviewed: May 11, 2020
Reviewed: May 9, 2022