SCHOOL DISTRICT INTERNET ACCESS FOR STAFF

Each employee is responsible for his/her actions and activities involving district computers, networks and Internet services, and for his/her computer files, passwords and accounts. These rules provide general guidance concerning the use of district computers and examples of prohibited uses. The rules do not attempt to describe every possible prohibited activity. Employees who have questions about whether a particular activity or use is prohibited are encouraged to contact a building administrator or the Network Administrator.

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 district computers will also result in referral to law enforcement.

Access to School Computers, Networks and Internet Services
The level of employee access to district computers, networks and Internet services is based upon specific job requirements and needs. With approval of the Network Administrator or Technology Curriculum Facilitator, an employee may install additional licensed software. Unauthorized access to secure areas of the district's computers and networks is strictly prohibited.

Acceptable Use
Oyster River School District computers, networks and Internet services are provided to employees for administrative, educational, communication and research purposes consistent with the district's educational mission, curriculum and instructional goals. All Board policies, district rules and expectations for professional conduct and communications apply when employees are using the school district's computers, networks and Internet services.

Personal Use
District computers, network and Internet services are provided for purposes related to school programs and operations, and performance of 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 other Board policy, procedure or school rules. "Incidental personal use" is defined as use by an individual employee for occasional personal communications.

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 district rules, including harassing, discriminatory or threatening communications and behavior; violations of copyright laws, etc. The school district assumes no responsibility for illegal activities of employees while using district computers.
2) Any use involving materials that are obscene, pornographic, sexually explicit or suggestive.
3) Any inappropriate communications with students or minors.
4) Any use for private financial gains, or commercial, advertising or solicitation purposes.

SCHOOL DISTRICT INTERNET ACCESS FOR STAFF *(Continued)*

5) Any use as a forum for communicating by e-mail or any other medium with other district 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 administrator.
6) Any communication that represents an employee's personal views as those of the school district or that could be misinterpreted as such.
7) Downloading or loading software or applications without permission from the Network Administrator. Unauthorized copying of software is illegal and may subject the copier to substantial civil and criminal penalties. The school district assumes no responsibility for illegal software copying by employees.
8) Mass e-mails may only be sent to school users or outside parties for official school purposes and with the permission of the building administrator.
9) Any malicious use or disruption of the school district'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 district'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 or circumvent the school district's filtering/blocking technology.
12) Failing to report a breach of computer security to the system administrator.
13) Using district computers, networks and Internet services after such access has been denied or revoked.
14) Any attempt to delete, erase or otherwise conceal any information stored on a district computer that violates these rules, other Board policies or school rules or refusing to return computer equipment issued to the employee upon request.
15) Storing personal files, photographs, music, etc. on district computers without the explicit approval of the Network Administrator. Personal files take up valuable network space that must be maintained as school-related data only.

No Expectation of Privacy
Oyster River School District computers remain under the control, custody and supervision of the school district at all times. The district 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 district computers, including e-mail, stored files and Internet access logs.

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.

SCHOOL DISTRICT INTERNET ACCESS FOR STAFF *(continued)*

Employee/Volunteer Responsibility to Supervise Student Computer Use
Employees and volunteers who use district 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 district'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 administrator.

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

Additional Rules for Use of Personally-Owned Computers by Employee

1. An employee who wishes to use a personally-owned computer in school must complete a Staff Personal Computer Registration and Agreement form. The form must be signed by the employee, the school principal or supervisor and the Network Administrator or Technology Curriculum Facilitator. There must be a legitimate work-related basis for any request.
2. The Network Administrator or Technology Curriculum Facilitator will determine whether an employee's personally-owned computer meets the district's requirements.
3. Requests may be denied if it is determined that there is not a legitimate work or education-related reason for the request and/or if the demands on the district's network or staff would be unreasonable.
4. The employee is responsible for proper care of his/her personally-owned computer, including any costs of repair, replacement or any modifications (including installation of up-to-date anti-virus software) needed to use the computer at school.
5. The district is not responsible for damage, loss or theft of any personally-owned computer.
6. Employees are required to comply with all Board policies, administrative procedures and school rules while using personally-owned computers at school. Employees are not allowed to access the district's network without specific authorization from a school administrator.
7. Employees shall not allow students to access their personal computers.
8. Employees have no expectation of privacy in their use of a personally-owned computer while it is being used at school.
9. Violation of these rules may result in the district confiscating any personally-owned computer used by an employee in school without authorization. The contents of the computer may be searched in accordance with applicable laws and policies.