COMPUTING RESOURCES

General Computer Use

The District's policy describes the proper use of the District's computer systems by all its employees, consultants, contractors, students, and patrons. The following list, while not exhaustive, provides guidelines for acceptable behavior and characterizes unacceptable behavior that may subject individuals to disciplinary action.

- Individuals shall only utilize authorized accounts, files, software, and computer resources.
- Individuals may not misrepresent their identity in any type of electronic communication.
- Individuals shall not violate the privacy of others. Violations of privacy include, but are not limited to, the access of accounts and files without consent and the monitoring of network communications explicitly meant for another.
- Offensive or objectionable material, e-mail, worldwide web pages, usenet news articles, etc. are prohibited and are not within the intended use of the system and network services. Furthermore, profane, offensive, and inflammatory speech and messages are also prohibited.
- Chain letters, broadcasting messages to individuals or lists of users, and other large distribution of personal messages interfere with the work of others and are not allowed.
- Individuals must not attempt to modify system configurations or account restrictions, or attempt to breach the District's computer security systems, regardless of intent. This includes the unauthorized installation or modification of software, firmware, etc.
- Individuals must not misuse the District's computing resources so as to reduce their efficiency or affect access to the detriment of others.
- The District's computer systems may not be used for commercial or profit making purposes without the prior written authorization of the Superintendent or designee.
- Computing resources may only be used with the restrictions of software access, license, and usage agreements. Individuals must not make or distribute unauthorized copies of copyrighted software.
- Individuals must take all reasonable precautions to prevent unauthorized access to accounts of data by others, both inside and outside the District.
- Individuals may be held liable for any/all costs that the District may incur as a result of their unauthorized system use.
- Computer accounts, passwords, and other types of authorization that are assigned to individual users should not be shared with others.
- Users should assign obscure password accounts and change them frequently.
- Users should be aware of computer viruses and other destructive computer programs, and take steps to avoid becoming victim or unwitting distributor.
- Non-instructional related computer games may not be played on District time.

- Violations of this policy will be handled in a manner consistent with comparable situations requiring disciplinary action. A system administrator may suspend or restrict a user's computing privileges during the investigation of a problem.
- A system administrator is authorized to access employees' computer files.
- If uncertain about a specific situation, individuals should consult Information Systems Services or Human Capital.
- Individuals are expected to report any violations, flaws, or other deficiencies in the security of the District's computer systems.

Security

The security of the District's computing assets and data is extremely important. To ensure the security of computing assets and data, the District has established the following guidelines:

- All reasonably available physical security measures will be taken to safeguard District computing resources.
- District computing resources should be secured by the user when not in use or when unattended.
- A computer logged into the District Wide Area Network (WAN) or the Internet should not be left unattended. Users are responsible for all transactions made under their user ID and password.
- All users having access to the District WAN or Internet will be assigned a user ID and a password. Safeguarding of the password will be the responsibility of the individual user. Individual users will be held responsible for safeguarding their passwords.
- The District has the right to restrict a user's access to the District WAN or the Internet by restricting the locations and workstations from which the user may log on, or by denying or limiting access to programs and files.
- The District administration may deny, revoke, or suspend specific user accounts for violation of these policies or procedures.

Electronic Mail (e-mail)

Ease of communication is extremely important in today's fast-paced environment. To that end, the District has installed electronic mail (e-mail) throughout the District. To ensure appropriate use of such systems, the District has established the following guidelines:

- E-mail hardware and software are considered to be District property. Additionally, all messages composed, sent or received on e-mail are and remain the property of the District. They are not the private property of any employee. Accordingly, employees should have no expectation of privacy with respect to such materials and information.
- The use of the e-mail is for the conduct of instruction and business on behalf of the District. Use of the system for reasons other than District business and instruction will be subject to scrutiny and corrective action if such use is deemed to be inappropriate or abusive.
- E-mail may not be used to solicit for commercial ventures, religious or political causes, outside organizations, or other non-job/class-related purposes.

- The e-mail system is not to be used to create offensive or disruptive messages. Among those considered offensive are messages which contain sexual implications, racial slurs, gender-specific comments, or any other comments that ridicule a person's age, gender, sexual orientation, race, religious or political beliefs, national origin, and/or disability.
- The e-mail systems shall not be used to send or receive copyrighted materials, trade secrets, proprietary financial information, or similar material without appropriate authorization.
- The District reserves and intends to exercise the right to review, audit, intercept, access, and disclose all messages created, received, or sent over the e-mail system for any purpose. The contents of e-mail properly obtained for legitimate business/instructional purposes may be utilized within the District without the permission of the employee or student.
- The confidentiality of any message should not be assumed. Even when a message is erased, it can still be retrieved and read. Further, the use of passwords for security does not guarantee confidentiality.
- Notwithstanding the District's right to retrieve and read any/all e-mail messages, such messages should be treated as confidential by other employees/students and accessed only by the intended recipient. Employees/students are not authorized to retrieve or read e-mail messages that are not sent to them. Any exception to these guidelines must be approved by the employee/student whose messages are being retrieved or read.
- Employees/students shall not use a code, access a file, or retrieve any stored information unless authorized to do so. Employees/students should not attempt to gain access to another employee's/student's messages without permission.
- Employees/students who discover a violation of this policy should notify Information Systems Services, their supervisor or Human Capital.
- Employees/students who violates this policy or uses the e-mail system for improper purposes shall be subject to corrective action, up to and including discharge/suspension.

District Standards

Computer hardware or software utilized within the District must comply with District standards. Information Systems Services will maintain standards for hardware and software and will update these as necessary.

Internet

Internet usage will be subject to the same General Computer Use policies and guidelines listed above. Additionally, a separate policy exists for Internet Protection.