SCHOOL DISTRICT OF JOHNSON CREEK BOARD OF EDUCATION POLICY	REFERENCE CODE: 363

Use of Computer Networks and District Technology Resources

The School District of Johnson Creek is committed to the appropriate and effective use of technology as a means for achieving its educational mission and goals. Technology, as defined to include stand-alone computers, local school area networks, wide area networks, telecommunication systems, the Internet, Intranet, and other technology devices, offers vast, diverse and unique educational resources. The District's purpose in providing access to technology to students, staff and other users is to promote educational excellence.

USE OF NETWORK RESOURCES

1. Ownership and Control

   The School District of Johnson Creek retains full ownership and control of all its technology equipment and resources. Any user files, communications, or other information stored on District equipment shall not be considered private. School administrators or the District's technology coordinator may review files and communications to maintain the integrity of network resources and ensure that users are in compliance with district policy, procedures and rules. The District will not be responsible for any damage or loss of data caused by its own negligence or user's errors/omissions and denies any financial obligations arising from unauthorized use of the network or technology resources. Moreover, the District shall not be responsible for the accuracy or quality of information obtained through its computer networks and technology resources. In addition, the Johnson Creek Board of Education reserves the right to modify its policy, procedures and rules as deemed necessary.

   CIPA (Children's Internet Protection Act)
   It is the Policy of the School District of Johnson Creek to: (a) prevent access to or transmission of inappropriate content by its computers and over its network through electronic mail or other forms of communication; (b) promote the safety and security of minors using the District's computers, electronic mail, and other forms of communications; (c) prevent unauthorized access (such as "hacking") and other unlawful activities, (d) prevent unauthorized online disclosure, use, or dissemination of student personally identifiable information; and (e) comply with CIPA-the Children's Internet Protection Act (Pub. L. No. 106-554 and 47 USC 254(h) and all other applicable laws.

   The District uses an Internet content filtering system to block access to material that is harmful to students, obscene or disruptive to the educational or work environment, and to a lesser degree, high risk activities. The District uses reasonable technology protection measures designed to comply with CIPA's requirements. The District reserves the right to block sites that do not enhance educational activities or are not in compliance with CIPA. No technology measure can block 100% of inappropriate content so the District emphasizes the

importance of responsible use and of parent and staff supervision in monitoring use of technology. Proxy sites may not be used to bypass Internet content filters.

2. User Privileges/Responsibilities

   Use of computer networks and District technology resources in the School District of Johnson Creek is a privilege, not a right. Use is to be for educational purposes only. All users will be expected to adhere to District policy, procedures and rules, all of which require efficient, ethical and lawful utilization. Users shall be responsible for damage and vandalism to the equipment, systems and software resulting from deliberate or willful acts. Illegal use of the networks, intentional deletion or damage to files or data belonging to others, copyright violations or theft of services will be reported to the appropriate legal authorities. Vandalism shall be defined as any intentional attempt to alter or destroy hardware, software, wiring, equipment connections, or the data of another user. This includes, but is not limited to the loading or creation of computer viruses. General rules of behavior and communication are expected when using the computer networks and the District's technology resource.

   The District recognizes that the Internet links users to uncensored information and ideas throughout the world, and there is potential for users to access information that is inconsistent with the mission and goals of the District. Even with a filtering system, complete control and/or access to objectionable material cannot be assured. Some independent users may still discover unsuitable information or have access to materials that are illegal, defamatory, inaccurate or potentially objectionable to some people. In addition, it is possible to purchase certain goods and services via the Internet which could result in unwanted financial obligations for which a student, parent or guardian would be liable. Ultimately, parents and guardians of minors will be responsible for setting and conveying standards that their children should follow when using Internet resources.

3. Acceptable User Rules

   A. General Use
      1. All student use of computer networks and District technology resources must be physically supervised by a school staff employee
      2. Students may only print materials for school related assignments, projects and research.

   B. Account Access
      1. No person may use, or attempt to use, any personal computer accounts other than his/her own assigned account. The negligence or naivete' of another user in revealing an account name and password does not confer authorization to use the account.
      2. An user should only access, or attempt to access, files in his/her own accounts, files which have been made accessible to him/her by the files' owner or files which have been made publicly accessible by the files' owner.
      3. Individuals are not to use privately owned software on District computers without first obtaining permission from the District's technology coordinator. All licensing requirements must be followed.
      4. Each account user is responsible for all computing activities involving his/her account

and shall be held liable for any misuse of that account.

5. No person may create or use software with the intent to impair computer or network operations or to disrupt classroom teaching and learning.

   *Any exception to the access policies stated above must be approved by the building principal.

C. Proper Use of Computing Resources
   1. The use of computer networks and District technology resources may not be used for any activity which is contradictory to the educational mission and goals of the School District of Johnson Creek.
   2. The use of computer networks and District technology resources may not be used for any activity which violates the District's policies, procedures and rules.
   3. Computer networks and District technology resources may not be used for any activities which intimidate, threaten or harass individuals. Such activities include, but are not limited to, using networks and resources to store, print or send obscene, slanderous or threatening messages.
   4. The use of computer networks and District technology resources may not be directed toward personal profit making or commercial purposes.
   5. No person may store or use programs on District-owned systems which violate or hamper another person's use of computing resources. Examples of such programs are ones which attempt to control terminals, obtain another user's password, acquire another user's files, circumvent system security measures or crash the computer system or harass users, etc. The devising and/or spreading of computer viruses is expressly forbidden.
   6. The use of computer games is strictly prohibited, except as supporting, classroom assignments or those that are publicly provided by the Instructional Media Center.
   7. Programs that allow the sending of anonymous mail, mail with altered headers, anonymous message or anonymous files are prohibited.

D. Use of Licensed Software

   1. No user is allowed to store or use private copies of licensed software (except that provided by the District) on any District computer system unless the user provides the building library media specialist with the original disks and a copy of the license agreement allowing such possession. The District assumes no responsibility for privately owned software.
   2. Stolen or bootleg copies of software are not allowed on any District computer.
   3. No user may copy, or attempt to copy, any proprietary or licensed software provided or installed by the District. This includes software on the District network as well as that provided for use on any District microcomputer.

E. Use of the Internet
   1. The purpose of the District's access to the Internet is to support research and education in and among academic institutions by providing access to unique resources and the opportunity for collaborative work. Transmission of any material in violation of any federal or state regulation is prohibited. This includes, but is not limited to

copyrighted material, threatening or obscene material or material protected by trade secret. The District's Internet access is to be used for educational purposes. Commercial use, including product advertisement or political lobbying, is prohibited.

2. The use of the Internet is a privilege, not a right. Inappropriate use shall result in the temporary or permanent suspension of Internet privileges. District staff may request the denial or temporary or permanent suspension of Internet privileges. District staff may request the denial or temporary or permanent suspension of specific user privileges. This action shall be taken in concert with the building administrator and the Technology and Information Services Director.
3. Persons using E-mail are expected to abide by the generally accepted rules of conduct. These include (but are not limited to) the following:
   (a) Be polite. Do not get abusive in messages to others.
   (b) Use appropriate language. Do not swear, use vulgarities or any other inappropriate language.
   (c) Illegal activities are strictly forbidden.
   (d) Do not reveal personal addresses or phone numbers of others.
   (e) Do not use the network in such a way that would disrupt the use of the network by other users.

   Messages relating to or in support of illegal activities may be reported to the authorities and may result in disciplinary action.
4. Attempts at unauthorized login to the Internet shall result in disciplinary action.

5. Penalties for Network and Technology Resource Violations

Violation of the District's policy, procedures and rules as related to computer networks and technology resources may result in loss of access as well as other disciplinary and/or legal action.

The District will cooperate fully with local, state and federal officials in any investigation concerning or relating to any illegal activities. In the event that there is an allegation that a student has violated the District's policy, procedures or rules, the student will be provided with notice of the alleged violation and an opportunity to present an explanation before the District terminates his/her use privileges.

Disciplinary actions will be tailored to meet the specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately. If the alleged infraction involves a violation of other provisions of the code of student conduct or other School Board policies and District regulations governing student discipline, the violation will be handled in accordance with the code of student conduct policy and its implementing regulations.

Employees violating District policy, procedures and/or rules are subject to disciplinary action by the superintendent or designee. Violations may subject the employee to disciplinary action up to and including dismissal, depending upon the nature of the violation. Violations of the policy will also be addressed by the technology coordinator who may, upon discussion with appropriate administration, terminate the system privileges of an employee by giving

written notice of the alleged violation and the opportunity to respond.

Prior to the use of any computer networks and District technology resources, a Consent Agreement must be signed indicating user willingness to abide by District policy, procedures and rules. Consent Agreements will be required to be completed when students enter kindergarten and again when they enter middle school and for the last time when they enter high school. New students to the district will be required to initially complete the Consent Agreement at the appropriate building level when they register. If the individual is a minor, the Consent Agreement must also be signed by a parent/guardian. All signed Agreements will be kept on file in the various building level offices or the District office. The School District of Johnson Creek will respect the right of parent(s)/ guardian(s) to decide whether or not to authorize computer networks and technology resource access for their child/children.

The District shall provide annual written notice of this policy to all employees, community users and students and their parents. Annually, staff shall discuss with all students the meaning of the District's policy regarding the use of computer networks and technology resources.

Adopted: 12/1/03
Reviewed: 7/31/08
Reviewed: 11/26/07
1st Reading: 3/19/2012
Revised: 4/16/12