COMPUTER/ONLINE SERVICES
(Acceptable Use and Internet Safety)

This document constitutes the District's Computer Network and Internet Acceptable Use policy ("Policy") and applies to all persons who use or otherwise access the Network and/or Internet, whether with District or personal equipment or whether on-site or by wireless or other remote access ("Users").

1. Definitions. For purposes of this Policy,

   A. "Network" means the District's group of interconnected via cable and/or wireless computers and peripherals, all other District software and hardware resources including all web-based material and all Web hosting, all data, databases and storage media, all standalone, portable and/or borrowed devices, and all provided connectivity between and among Users and from Users to the global Internet, including any and all Instructional Technology Centers or other third-parties providing connectivity and other services, and any and all identifiers, accounts, rights, permissions, and current or future hardware, software or connectivity owned or managed by the District to which access is provided to Users. Individual system computers are considered to be part of the "Network" and are subject to the terms of this Policy even when the User is not attempting to connect to another computer or to the Internet.

   B. "Use" of the Network means any and all actions of a User which create traffic on the Network, including traces or remnants of traffic that pass through District equipment, wiring, wireless networks or storage devices regardless of any other factor such as passage of time, user deletion, transit of the Network without storage or origination and/or storage on personal equipment.

2. Purpose and Use: The District is providing Users access to its Network to support and enhance the educational experience of students and to facilitate work duties of employees. Access to system computers and the Network is a privilege, not a right. The District reserves the right to withdraw access at any time for any lawful reason. The District reserves the right to determine what constitutes an improper use of system computers or the Network, and is not limited by the examples of misuse given in this Policy. Users may violate this Policy by evading or circumventing the provisions of the Policy, alone or with others. If Users have any doubt about their obligations under this Policy, including whether a certain activity is permitted, they must consult with their building principal to be informed whether or not a use is appropriate.

3. Users Bound by Policy in Accepting Access: The User consents to the terms of this Policy whenever he/she accesses the Network. Users of the Network are bound to the terms of this Policy regardless of whether or not a copy was received and/or signed for by the User.

4. Personal Responsibility: Users are responsible for their behavior on the Network just as they are in a classroom, school hallway or other District property. Each User is responsible for reading and abiding by this Policy and any and all future amendments, which will be made readily available in both electronic and printed form. Anonymous use is not permitted and access (including passwords) may not be shared or transferred. If a User suspects that a password is not secure, he/she must inform Technology Services immediately. Any improper use of your account, even if you are not the User, is your responsibility.

5. Reporting Misuse of the Network: Users must report any misuse of the Network to their building principal. "Misuse" means any apparent violation of this Policy or other use which has the intent or effect of harming another person or another person's property.

6. Violating Policy with Personal Equipment: The use of personal equipment and/or personal Internet access to violate this Policy or to assist another to violate the Policy is prohibited. Exceeding permission (such as abusing access to unfiltered Internet connectivity) is a violation of this Policy. Using private equipment to divert student time and/or attention from scheduled educational activities, or to divert paid work time from its proper purpose, is always strictly prohibited. Personal equipment used to violate this Policy on school property is subject to search related to the violation and seizure for a period of up to 30 days.

7. Discipline for Violation of Policy: Violations of each of the provisions of this Policy are considered violations of the Student Code of Conduct (or if an employee, of the contract of employment), and each violation is a separate infraction. Violations may result in disciplinary action for students up to and including suspension or expulsion and/or referral to law enforcement, or up to termination and referral to law enforcement for employees. The District reserves the right to seek reimbursement of expenses and/or damages arising from violations of these policies. Disciplinary action relating to employees is always subject to the provisions of any applicable collective bargaining agreement.

8. Waiver of Privacy: By accepting Network access, Users waive any and all rights of privacy in connection with their communications over the Network or communication achieved through the use of District equipment or software. Electronic mail (email) and other forms of electronic communication (including instant messaging of all forms and SMS messages originating from email) are not guaranteed to be private.

The District owns all data in the system. Systems managers have access to all messages for purposes of monitoring system functions, maintaining system efficiency and enforcing computer/network use policies and regulations, District policies, and State and Federal laws. Illegal activities or suspected illegal activities may be reported to the authorities.

9. Confidentiality and Student Information: Users are responsible for maintaining security of student information and other personally identifiable data that they access, even if they access such data accidentally or without permission, and for upholding FERPA (20 U.S.C. 1232 g), the student confidentiality law (Ohio Revised Code) and any other applicable privacy policies and regulations. Users are responsible whether such data is downloaded from the Network to their computer screen, transmitted by email, stored on a flash drive, portable device or laptop, copied by handwriting or by any or all other devices, forms of storage or methods. Negligence with respect to protecting the confidentiality of such data is considered a violation of this Policy whether or not such negligence results in identity theft or other harm.

10. District-Owned Equipment: Desktop computers, laptops, portable devices and other equipment belonging to the District are your responsibility. Any misuse, failure, damage or loss involving such equipment must be reported to Technology Services. Periodic maintenance on laptops and other hardware is required. It is your responsibility to make such equipment timely available for maintenance at the request of Technology Services. You may be held financially responsible for the expense of any equipment repair or replacement.

11. Unacceptable Uses of the Network: All Users must use the Network in an appropriate and responsible way, whether their specific actions are described in this Policy or not. Examples of unacceptable uses include, but are not limited to, the following:

    A. Offensive or Harassing Acts: Creating, copying, viewing, transmitting, downloading, uploading or seeking sexually explicit, obscene or pornographic materials. Using language inappropriate to the school environment, including swearing, vulgarities or language that is suggestive, obscene, profane, abusive, belligerent, harassing, defamatory, or threatening. Making, distributing or redistributing images, jokes, stories or other material that would violate this Policy or the District's harassment or discrimination policies, including material that is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, sexual orientation or other protected characteristics. Engaging in harassment, stalking or other repetitive unwanted communication or using the Internet in support of such activities.

B. Violations of Privacy: Unauthorized copying, modifying, intruding or attempts to copy, modify or intrude, into the folders, files, data, work, networks, passwords or computers of others, or intercepting communications intended for others. Copying, downloading, uploading or transmitting student or District confidential information.

C. Creating Technical Problems: Knowingly performing actions that cause technical difficulties to the system, other users or the Internet. Attempting to bypass school Internet filters or to "hack" into other accounts or restricted information. Uploading, downloading, creating or transmitting a computer virus, worm, Trojan horse or other harmful component or corrupted data. Attempting to hack, alter, harm, destroy or interfere with the normal operation of software, hardware, data, other District Network resources, or using the District Network or to do any of the same acts on the Internet or outside Networks. Downloading, saving and/or transmitting data files large enough to impede the normal functioning of the computer or the Network (such as many music, video, image, or other software files) unless given permission by the District Technology Coordinator. Moving, "repairing, " reconfiguring, reprogramming, modifying or attaching any external devices to Network equipment, computers or systems without the permission of the District Technology Coordinator. Removing, altering or copying District software for personal use or for the use of others.

D. Use of Outside Services: All email, document storage, blogs or any and all other services must be provided by the District on its Network. The use of other providers of such functionality or storage through the Network is prohibited. Outside email systems may be used for personal email, subject to the loss of privacy rights as stated in this Policy. No District business shall be conducted on outside email services unless a copy of each such communication is copied or forwarded to the User's District account for archiving. Outside document storage, such as Google Docs, and other services, such as blog hosting, may be used with the permission of the District Technology Coordinator, subject to an evaluation of student privacy.

E. Violating Law: Actions that violate State or Federal law or encourage others to do so. Offering for sale or use, soliciting the purchase or provision of, or advocating the use of any substance that the possession or use of is prohibited by law or District Policy. Seeking information for the purpose of creating an explosive device or biohazard, or communicating or seeking materials in furtherance of criminal activities, terrorism or other threatening acts.

F. Violating Copyright: Uploading, downloading, copying, redistributing or republishing copyrighted materials without permission from the owner of the copyright. Users should assume that materials are protected under copyright unless there is explicit permission for use.

G. Personal Use: Personal shopping, buying or selling items, soliciting or advertising the sale of any goods or services, or engaging in or supporting any kind of business or other profit-making activity. Interacting with personal websites or other social networking sites or tools that are not part of an educational or work project, receiving or posting messages to websites or other social networking or blog sites not part of an educational or work project, participating in any type of gaming activity, engaging in social or hobby activities or general recreational web browsing if such browsing occurs during instructional time or designated work time.

H. Political Use: Creating, transmitting, or downloading any materials that support or oppose the nomination or election of a candidate for public office, soliciting political contributions through the Network or conducting any type of official campaign business.

I. General Misconduct: Using the Network in a manner inconsistent with the expectations of the schools for the conduct of students and employees in the school environment. Uses that improperly associate the District with Users' personal activities or to activities that injure the District's reputation. Uses that mislead others or violate the standards of academic or personal integrity, including but not limited to plagiarism, disseminating untrue information about individuals or groups, or using another's password or some other user identifier.

12. Specific Limits on Communication Over the District Network:

Expressing Opinion: The Network has been created at public expense and exists for purposes relating to education and administration. It does not exist to serve as a personal blog for the expression of opinions or as a public forum of any kind. It is not the intention of the District to allow the public, staff or students to use the Network, including the web hosting or linking ability, for purposes of expressions of private opinions, or to support private or public causes or external organizations.

Large Group Mailings: The sending of messages to more persons than is necessary for educational or school business purposes is a misuse of system resources and User time. Large group mailings, such as "all District" or "all building" are reserved for administrative use, subject to any exceptions that may be developed by the administration or the District Technology Coordinator. Users may not send emails to more than 10 recipients in a single message, subject to exceptions developed by the administration or the District Technology Coordinator. The District Technology Coordinator may also develop specific limitations on the use of graphics, the size, number and type of attachments, and the overall size of email messages sent on the system. The use of multiple messages, non-system addresses or other technique to circumvent these limitations is strictly prohibited.

Personal Email. Limited personal use of District email by employees to communicate with family, friends and colleagues who are willing recipients is permitted as a personal convenience, but must not impact paid work time and is subject to all of the provisions of this Policy. Misuse of the privilege is prohibited, and includes but is not limited to excessive volume, frequency, inappropriate content, mailing to unwilling addressees, or uses that may bring the District into disrepute. Violations will be determined in the sole discretion of the Superintendent. "Limited personal use" is defined as no more than 10 messages during any one day, with no attachments large enough to impede the normal functioning of the computer or the Network, as determined by the District Technology Coordinator. Exceptions to this limitation may be permitted for personal emergencies and other extenuating circumstances.

Electronic Signatures: Users shall not legally verify documents or use electronic signatures in any way unless they have been trained in an approved verification or signature system approved by the administration. Users asked to legally verify or electronically sign documents should report the situation to their building principal.

13. System Security and Integrity: The District reserves the right to suspend operations of the Network, in whole or in part, at any time for reasons of maintaining data security and integrity or any other lawful reason. The District reserves the right to block or filter any websites, email addresses, servers or Internet domains which it, in its sole judgment, has determined to present a risk of exposing students or employees to sexually explicit or otherwise inappropriate content, or which exposes the system to undue risk of compromise from the standpoint of security or functionality.

    The District has implemented technology-blocking measures to prevent students from accessing inappropriate material or materials considered to be harmful to minors on school computers. The District has also purchased monitoring devices that maintain a running log of Internet activity, recording which sites a particular user has visited.

    "Harmful to minors" is defined as any picture, image, graphic image file or other visual depiction that:

    A. taken as a whole and with respect to minors appeals to a prurient interest in nudity, sex or excretion;

    B. depicts, describes or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts or lewd exhibition of genitals or

    C. taken as a whole lacks serious literary, artistic, political or scientific value as to minors.

    The District will educate minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyber-bullying awareness and response. The Superintendent/designee will develop a program to educate students and these issues.

14. No Warranties Created: By accepting access to the Network, you understand and agree that the District, any involved Information Technology Centers and any third party vendors make no warranties of any kind, either express or implied, in connection with provision of access to or the use of the Network. They are not responsible for any claims, losses, damages or costs (including attorneys' fees) of any kind suffered, directly or indirectly, by any student or employee arising out of that User's use of and/or inability to use the Network. They are not responsible for any loss or deletion of data; they are not responsible for the accuracy of information obtained through electronic information resources.

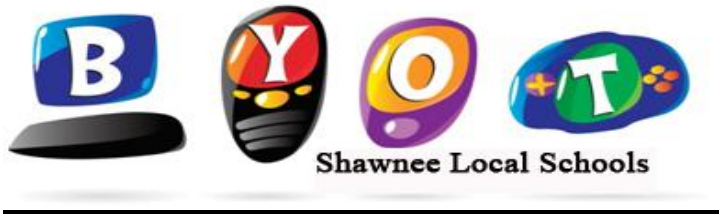
15. Updates to Account Information: You must provide new or additional registration and account information when asked in order for you to continue receiving access to the Network. If, after you have provided your account information, some or all of the information changes, you must notify your building sysop to receive this information.

16. Records Retention and Production: Users must comply with all District directions regarding the retention and management of email or documents. The District retains the right to receive a copy of a record from an Employee User's private computer if for some reason it exists only on that computer.

[Adoption date: September 25, 2012]

LEGAL REFS.: U.S. Const. Art. I, Section 8
Family Educational Rights and Privacy Act; 20 USC 1232g et seq.
Children's Internet Protection Act; 47 USC 254 (h)(5)(b)(iii); (P.L. 106-554, HR 4577, 2000, 114 Stat 2763)
ORC 3313.20
3319.321

CROSS REFS.: AC, Nondiscrimination
ACA, Nondiscrimination on the Basis of Gender
ACAA, Sexual Harassment
EDEB, Bring Your Own Technology(BYOT)Programs
GBCB, Staff Conduct
GBH, Staff-Student Relations (Also JM)
IB, Academic Freedom
IIA, Instructional Materials
IIBH, District Websites
JFC, Student Conduct (Zero Tolerance)
JFCF, Hazing and Bullying (Harassment, Intimidation and Dating Violence)
Staff Handbooks
Student Handbooks



Protocol for the Use of Technology on/off SLSD Campus

As new technologies continue to change the world in which we live, they also provide many new and positive educational benefits for classroom instruction. To encourage this growth, students may now bring their own technology. B.Y.O.T will be evaluated with student and staff participation in the monthly Administrative meetings.

Definition of "Technology"
For purposes of BYOT, "Technology" means a privately owned wireless and/or portable electronic hand held equipment that includes, but is not limited to, existing and emerging mobile communication systems and smart technologies, tablet pc's, portable internet devices, Personal Digital Assistants (PDAs), hand held entertainment systems or portable information technology systems that can be used for word processing, wireless Internet access, image capture/recording, sound recording and information transmitting/receiving/storing, etc.

Internet
Only the internet gateway provided by Shawnee Local Schools may be accessed while on campus. Personal internet connective devices such as but not limited to cell phones/cell network adapters are not permitted to be used to access outside internet sources at any time.

Security and Damages
Responsibility to keep the device secure rests with the individual owner. **Shawnee Local School District and its employees are not liable for any device stolen or damaged on campus.** If a device is stolen or damaged, it will be handled through the administrative office similar to other personal artifacts that are impacted in similar situations. It is recommended that skins (decals) and other custom touches be used to physically identify your device from others. Additionally, protective cases for technology are encouraged.

B.Y.O.T. Shawnee Local Schools Student Agreement
The use of technology to provide educational material is not a right but a privilege. A student does not have the right to use his or her laptop, cell phone or other electronic device while at school. When abused, privileges will be taken away. When respected, they will benefit the learning environment as a whole.

Students and parents/guardians participating in B.Y.O.T. must adhere to the Student Code of Conduct, as well as all Board Policies, particularly Internet Acceptable Use (Board Policy EDE) and Internet Safety (Board Policy EDE). Additionally, technology:

- Must be in silent mode while on school campuses and while riding school buses.
- Must be used at appropriate times in accordance with teacher instructions. The devices must not be a distraction for the student or those around him/her nor be a source of any classroom disruption.
- May not be used to cheat on assignments or tests, or for non-instructional purposes (such as making personal phone calls and text/instant messaging).
- May not be used to record, transmit or post photographic images or video of a person, or persons on campus during school activities and/or hours.
- May only be used to access files on computer or internet sites which are relevant to the classroom curriculum. Students acknowledge that:
- "Cyber-bullying" is when a child, preteen or teen is tormented, threatened, harassed, humiliated, embarrassed or otherwise targeted by another child, preteen or teen using the Internet, interactive and digital technologies or mobile phones. School officials will address issues within the schools jurisdiction as outlined in the student handbook.
- The student is responsible for knowing how to properly and effectively use their device and this should not be a burden for the teachers or technology staff.
- All devices must only connect to Shawnee Local School District's wireless network. All cellular or other wireless networking that does not include SLSD filter must be disabled.
- Bringing on premises or infecting the network with a Virus, Trojan, or program designed to damage, alter, destroy, or provide access to unauthorized data or information is in violation of Board Policy EDE.
- Processing or accessing information on school property related to "hacking", altering, or bypassing network security policies is in violation of Board Policy EDE.
- The school district has the right to collect and examine any device that is suspected of causing problems or was the source of an attack or virus infection.
- Shawnee Local School District reserves the right to ask any guest user to discontinue the use of their personal technology for any reason.
- Personal technology is charged prior to bringing it to school and runs off its own battery while at school.
- Teachers reserve the right to utilize or not utilize the use of devices and will determine implementation on an individual basis.

I understand and will abide by the above policy and guidelines. I further understand that any violation is unethical and may result in the loss of my network and/or technology privileges as well as other disciplinary action.

_____ _____

Signature of Student Date

_____ _____

Signature of Parent/Guardian Date

[Adoption date: September 25, 2012]

LEGAL REFS.: U.S. Const. Art. I, Section 8
Family Educational Rights and Privacy Act; 20 USC 1232g et seq.
Children's Internet Protection Act; 47 USC 254 (h)(5)(b)(iii); (P.L. 106-554, HR 4577, 2000, 114 Stat 2763)
ORC 3313.20
3319.321

CROSS REFS.: AC, Nondiscrimination
ACA, Nondiscrimination on the Basis of Gender
ACAA, Sexual Harassment
EDEB, Bring Your Own Technology (BYOT) Programs
GBCB, Staff Conduct
GBH, Staff-Student Relations (Also JM)
IB, Academic Freedom
IIA, Instructional Materials
IIBH, District Websites
JFC, Student Conduct (Zero Tolerance)
JFCF, Hazing and Bullying (Harassment, Intimidation and Dating Violence)
Staff Handbooks
Student Handbooks