Responsible Use of School Technology for University Schools

1. Statement of University Schools and Ball State University Policy.

   The Policy of University Schools and Ball State University is to provide technological resources to students and employees for the purpose of promoting the efficient operation of University Schools and University, advancing student achievement, and permitting students and employees to acquire 21st century skills. University Schools and Ball State University expect employees and students to utilize technologies and facilities provided in a manner consistent with this policy.

2. Scope of this Policy

   This Policy applies to all technology provided University Schools and Ball State University, in addition to students' and employees' own personal devices (collectively "users"). This includes, but not limited to telephones, cell phones, digital media players, PDAs, laptop and desktop computers and work stations, direct radio communication, pagers, internet access, voice mail, email, text messaging, facsimile transmission and receipt, and any computer based research and/or communication

3. Definition of Terms Used in This Policy

   As used in this policy:

   "Confidential Information" means information that is declared or permitted to be treated as confidential by state or federal law or School Policy on access to public records.

   "Proprietary information" means information in which a person or entity has a recognized property interest such as copyright.

   "Personal device" includes but not limited to cell phones, smart phones, laptops, slates, handhelds or any other device that is not the property of University Schools and Ball State University, but is used in or on school property, in or on property that is being used by the school for a school function, or used anywhere and connected to University Schools or Ball State University technology by a wired or wireless link.

   "System Administrator" means the University Schools employee designated by the Superintendent to maintain and/or operate the school's technology and network.

"Technology" includes but not limited to computers and computer systems, public and private networks such as the Internet, phone networks, cable networks, voice mail, e-mail, telephone systems, copiers, fax machines, audio-visual systems, cell phones, PDA's, laptop and desktop computers, direct radio communications, pagers, text messaging and similar equipment as may become available.

"User" means a School employee, student, volunteer or other person that uses technology associated with University Schools.

4. Violation of this Policy

    a. Intentional, knowing, and reckless or negligent violations of this Policy may result in denial of further access to technology, suspension or expulsion of students, and discipline of employees including suspension without pay or termination of employment. Such a violation by a person affiliated with a contractor or subcontractor rendering services to the school may result in cancellation of the contract of the contractor or subcontractor
    b. A user observing or learning of a violation of this policy is required to report the violation of this policy to the user's immediate supervisor (for employees or volunteers) or teacher (for students).
    c. University Schools and Ball State University prohibit taking negative action against any employee for reporting a possible deviation from this policy or for cooperating in an investigation. Any employee who retaliates against another employee for reporting a possible deviation from this policy or for cooperating in an investigation will be subject to disciplinary action, up to and including termination. This policy is not intended to prevent employees from engaging in discussions regarding their wages, hours, or working conditions with any other employee or engaging in protected concerted activity. Employees will not be disciplined or retaliated against for such discussions.

5. Ownership of University Schools and Ball State University Technology and Information

    a. The Technology provided by the school and all information stored by that technology is at all times the property of the School, subject to the copyright interest of an author. Documents and other works created or stored on the school technology are the property of University Schools and Ball State University and are not the private property of the user. This includes all information created using technology and/or placed on a website, blog and or other storage device.
    b. A user's history of use and all data stored on or sent to or from school technology shall at all times be subject to inspection by the System Administrator or a designee without notice to the user before or after

the inspection. The System Administrator may deny, revoke, or suspend a user's account and or access to school-provided technology.

c. Before being given access to school technology, each user shall be required to agree that they have read, understand, and agree to be bound by the following standards and condition for responsible use of that technology:
    i. They will comply with all conditions for the responsible use of school technology established by the school, System Administrator, or Superintendent.
    ii. They will notify a System Administrator if they have violated the conditions established for the use of school technology or have witnessed or become aware of another user misusing school technology. Users shall be responsible for noting and reporting any inappropriate use of school technology in violation of school policy or conduct standards including threats, bullying, harassment or communications proposing or constituting a violation of the law or the student code of conduct.
    iii. They shall not have an expectation of privacy in any use of school technology or the content of any communication using that technology other than a live telephone call, and the System Administrator or a designee may monitor their use of technology without notice to them, and examine all system activities a user participates in including but not limited to, email and recorded voice and video transmissions, to ensure proper and responsible use of the school's technology. Monitoring shall include the use of voicemail but shall not include monitoring a live communication between two or more parties unless at least one user is aware of the monitoring.
    iv. The user's history of use and any information or document accessed or stored on school technology is subject to inspection by the System Administrator or a designee and is subject to production pursuant to the Indiana Access to Public Records Act Ind. Code 5-14-3, subject to the decision of the System Administrator or Superintendent to claim a permissive or mandatory exemption to disclosure under the statue.
    v. They shall not have an expectation that data in any form created, maintained, transmitted or stored in or school technology will be maintained for any specific period of time, protected from unauthorized access or deleted from the system or storage when the user deletes the information from their account.
    vi. If they make use of a password, code or encryption devices to restrict or inhibit access to electronic mail or files, they will provide access to that information when requested to do so only the user's supervisor or the System Administrator. This

includes personal technology brought to or accessed during work or student day or at a school activity including bus transportation. The System Administrator or a designee shall be authorized to override any password or encryption device to access the technology.

vii. A user's information stored on school technology will not be stored beyond student graduation or volunteer and employee separation.

6. Investigation of Potential Violations of this Policy

    a. Students- If the System Administrator has a reasonable belief that a student has violated this policy or additional rules promulgated by the System Administrator and approved by the Superintendent, the System Administrator or a designee may investigate to determine if a violation has occurred. The results of the investigation shall be reported by email or in person, and the System Administrator shall take appropriate action.
    b. Employee and Volunteers- If a System Administrator has a reasonable belief that an employee or volunteer has violated this policy or additional rules promulgated by the System Administrator and approved by the Superintendent, the System Administrator or a designee may investigate to determine if a violation has occurred. If 1a System Administrator does not do the investigation, the results of the investigation shall be reported to a System Administrator by email or in person and the System Administrator shall take appropriate action.
    c. Appeals- A decision by a System Administrator in response to an investigated allegation of a violation this policy or additional rules promulgated by the System Administrator and approved by the Superintendent may be appealed in writing to the Superintendent. The Superintendent must receive a written appeal within five (5) instructional days after the System Administrator's decision has been issued. The Superintendent's decision concerning continued access to school technology and any other penalty shall be final.

7. Standards for Responsible Use of Technology

    a. Technology users have the same responsibilities while using technology that are expected in any other school activity. Responsible use of technology is ethical, academically honest, respectful of the rights of others, and consistent with the school's mission. Students to learn and communicate in correlation with the curriculum while under a teacher or supervisor's direction should use technology. Student owned personal devices and school technology shall be used

by students under school supervision with the objective of improving instruction and students learning.

b. Users must respect and protect the privacy intellectual property rights of others and the principles of their school community.
c. The privilege of use of school technology access and personal devices come with personal responsibilities for each user. Access is not a right and is provided on the condition that the user complies with this policy and any additional rules promulgated by the System Administrator and approved by the Superintendent. Use of school or personal technology on school property or for school purposes must be consistent with the educational mission and objectives of University Schools and Ball State University. Misuse of school technology and personal devices may result in sanctions and civil and criminal penalties.
d. The System Administrator is authorized to select, adopt and endorse the use of specific web based resources for teacher and student use. This may include resources for web site creation, multi media projects, presentations and other collaborations. The system Administrator in consultation with the other Superintendent designees will select resources based upon online safety, coordinated professional development, and informed technical support. If an employee, volunteer, or student desires to use an alternate resource, they may make written request to the System Administrator who will consult with the Principal or designee.
e. Any recording made on school grounds without written permission of the System Administrator is subject to copyright laws and the protection of the privacy rights of others, including personally identifiable information about a student protected by the Family Education Rights and Privacy Act ("FERPA"). Any recording, data or image in violation of this standard may be confiscated and deleted by the administrator. Any use of a personal device to record or invade the privacy of another person will result in sanctions for the person making the recording, as well as potential civil and criminal penalties.

8. Conditions & Standards for Responsible Student Use of School Technology.

The following apply to all student use of School Technology.

a. Creation of a web user ID by a student must be under the supervision of school personnel for the purpose of an assignment.
b. Students shall not be required to divulge personal information for access to a non-district managed technology.
c. Students will be permitted access to the Internet through school technology unless a parent/guardian has signed and returned a "Student Electronic Resources Restriction Form" during the current school year.

d. Students' use shall be filtered to minimize access to inappropriate materials. Student's access to inappropriate materials despite the presence of the filter shall be reported immediately to the System Administrator. The filtering software shall not be disabled or circumvented without the written authorization of a system administrator.
e. Users should expect monitoring of Internet access by the designees of a System Administrator. However, there is no guarantee that all student access will be monitored.
f. While online, student users should not reveal personal information such as name, age, gender, home address or telephone number, and are encouraged not to respond to unsolicited online contacts. Students should report to a teacher or supervisor any online contacts that are frightening, threatening, or inappropriate.
g. Students, parents and employees are advised that any student connection to any internet or network provider not under school control may not be properly filtered, at least to the same degree as connection through school provided access. The school is not responsible for the consequences of access to the sites or information through resources that circumvent the school's filtering software.

9. Condition & Standards for Responsible Use of School Technology Applicable to All users.

   The following apply to all users of school technology including students, employees and volunteer:
   a. Users will demonstrate legal and ethical behavior at all times when using school technology.
   b. Users will become familiar with and follow all applicable laws, including copyright laws and fair use guidelines.
   c. Users will become familiar with and comply with all expectations of the school for the responsible use of technology as communicated in school handbooks, policies, and other communications and standards concerning the use of technology.
   d. Users accessing the Internet through personal devices to school technology do so at their own risk. The School is not responsible for damages to hardware or software as a result of the connection of personal devices to school technology.
   e. Users should not knowingly transmit a computer virus or other malware that is known by the user to have the capability to damage or impair the operation of school technology, or the technology of another person, provider, or organization.

Failure to follow these conditions and standards may result in disciplinary action, up to and including expulsion for students and termination for employees.

10. Protection of Proprietary and Confidential Information Communicated or Stored on School Technology.

    a. Users of the School Technology are expected to protect the integrity of data, personal privacy, and property rights of other person when using school technology. Confidential information should never be transmitted or forwarded to or through a person not authorized to receive information.
    b. Any user communicating using school technology shall be responsible for knowing what information is confidential under law or school policy, and the transmission of confidential information in error may result in discipline of the user transmitting the confidential information.
    c. The practice of using distribution lists to send information shall not excuse the erroneous disclosure of confidential information. Users shall determine that distribution lists are current and review each name on any lists before sending confidential information, including but not limited to personally identifiable information about students protected by the Family Education Rights and Privacy Act ("FERPA")
    d. Users should not access confidential information in the presence of others who do not have authorization to have access to the information. Confidential information should not be left visible on the monitor when a user is away from the monitor. Confidential information should not be stored on personal devices that are not password protected.
    e. User should not copy, file share, install or distribute any copyrighted material such as software, database files, documentations, articles, music, video, graphic files, and other information, unless the user has confirmed in advance that the school has a license permitting copying, sharing, installation, or distribution of the material from the copyright owner. Violation of the right of a copyright owner may result in discipline a student, volunteer or employee, and may subject the violator to civil and criminal penalties.
    f. Users should not upload confidential information including personally identifiable information about students protected by FERPA, to any web-based external "cloud" service provider, unless the System Administrator has approved the use of the web-based external service provider.

11. Security of School Technology.

    a. Security on any school technology is a high priority when the resource involves many users and contains proprietary and confidential information. A user shall immediately notify the System Administrator if a security issue is identified. A security issue shall not be disclosed

or demonstrated to other users except in the presence of the System Administrator or a designee.

b. A user shall never use another user's password, or account, even with the permission from the user. Any need to have access to another's user's account should be addressed to the System Administrator or a designee.
c. An unauthorized attempt to log on to school technology as a System Administrator will result in cancellation of the user's access to School technology and may result in more severe discipline, up to and including termination for employees and expulsion for students.
d. A user identified as a security risk based upon one or more violations of this Policy may be denied access to all school technology. A decision denying or restricting a user's access may be appealed in writing to the Superintendent or a designee within ten (10) calendar days after written notice of the System Administrator's decision to the user. The decision of the Superintendent shall be final.

12. Incurring Fees for Services

No user shall allow charges or fees for services or access to a database to be charged to the school except as specifically authorized in advance of the use by System Administrator. A fee or charge mistakenly incurred shall be immediately reported to the System Administrator. Incurring fees or charges for services to be paid by the school for personal use or without prior authorization from the System Administrator may result in discipline including suspension or expulsion of a student, or suspension without pay or termination of an employee.

13. Training

All students and staff who work directly with students shall receive annual training on social media safety, cyber bullying, and appropriate responses.

Reviewed by Burris Advisory Council: July 28, 2014
Approved by the Dean of Teachers College: July 29, 2014
Implemented: August 2014