TECHNOLOGY RESPONSIBLE USE

The Salem School Board provides students and staff access to many types of technology resources. These resources provide opportunities to enhance learning and improve communication within our schools and community and beyond. The privilege of access requires students, teachers, staff and the public to exercise appropriate personal responsibility in the use of these resources. To this end, there should be no expectation of privacy among students, faculty, other staff, or guests availing themselves of the district’s electronic resources. Access is provided to assist users in the performance of their jobs or learning. Further, the computer system belongs to the school district to support its business and education purposes.

Introduction
This Responsible Use Policy was adopted by the Salem School Board to provide students, parents, faculty and staff with an overview of resources, expectations, and compliance requirements for technology use within the Salem School District (SSD). Students, parents, faculty and staff must read and sign the applicable section(s) of the Consent and Permissions Form at the end of this document, to acknowledge they understand and accept the policy.

Purpose
The District encourages and supports the use of technology to assist in preparing students for continuing education and careers. The District provides access to a wide range of technology to support learning, enhance student engagement, and assist students, faculty and staff in acquiring new skills. Technology is also used to improve administrative processes and communication with the wider Salem community.

Policy Review and Updates
Students, parents, faculty and staff will be presented with a policy for review and signature annually.

Definitions
User: anyone who accesses the district network

District network: any system or service owned, leased, or contracted by the SSD that supports the ability of users to access and use any digital resource, including but not limited to; the Internet and related services, including Google Apps for Education, and similar websites; applications running on SSD servers, file storage, email, printers, and peripheral devices.

Devices: any SSD owned or leased, student-owned, faculty-owned, staff-owned, or guest-owned equipment used to connect to the SSD network or SSD owned or leased equipment taken home by a student, teacher or staff member.

Guest: anyone that accesses the district network and isn’t a current student or employee.

Educational use: a use that supports learning, research and communication.

Limitations/Liabilities
Technology is constantly changing and not all circumstances can be anticipated or addressed in this policy. However, users are expected to understand and comply with both the “letter” and the “spirit” of this policy and show good judgment in the use of the resources provided. Users are expected to comply with all federal, state and local laws.

The SSD makes no warranties of any kind, implied or expressed, that the services and functions provided through the district network, or devices will be error free or without defect. The SSD is not responsible for damages users may suffer, including but not limited to loss of data or interruption of service.
The SSD is not liable for the actions of anyone connecting to the Internet through the district network. All users assume full liability, legal, financial, or otherwise, for their actions while connected to the Internet.

**Expectation of Privacy**

Users do not have an expectation of privacy in anything they create, store, send or receive on the district network and devices. The school district’s IT Department monitors the use of the district network to protect its integrity and optimal operation. Members of the SSD IT Department have full access to the district network and devices and may need to access/manage them as part of their duties. Routine maintenance and monitoring may lead to discovery that a user has violated this policy, other School Board policies, or federal, state or local laws. The school district reserves the right to inspect, copy, and review, all usage of the district network, and information sent or received in connection with this usage.

The district is a public entity subject to laws regarding public records and their disclosure. Accordingly, users must understand that some emails, Internet logs, and other district documents and electronic records may be accessed by third parties, including Internet service providers, and may be subject to disclosure upon a public records request or be disclosed to the general public under certain circumstances.

**Consequences for Violation**

Enforcement of this policy requires community support. Students, faculty or staff, that become aware of a violation of any portion of this policy, must immediately notify their building administrator. The building administrator will then notify the Director of IT. Violation of any portion of this policy can result in loss of access and may result in additional disciplinary or legal action. Disciplinary action for students who violate this policy may include suspension and expulsion. Disciplinary action for faculty or staff who violate this policy may include suspension and dismissal. All disciplinary action will be imposed in accordance with the appropriate disciplinary procedures and policies.

**Use Guidelines**

The district network is a resource provided and maintained for educational use. “Educational use” as used in this policy, for students means that students may only use the district’s technology for the purpose of their education, class work and district extra-curricular activities. “Educational use” as used in this policy, for staff means that staff may only use the district’s technology for the purpose of fulfilling their job duties. Use of the district network or related devices for unauthorized commercial work, product advertisement, or political lobbying is prohibited.

Users may not attempt to damage or to degrade the network’s performance. Users may not attempt to circumvent security systems, exploit or probe for security vulnerabilities, nor attempt any such activity against other systems accessed through the district network. Execution or compilation of programs designed to breach system security is prohibited unless authorized in advance. SSD IT reserves the right to terminate access, at any time, to anyone whose use of its resources violates the law or threatens system or network security, performance, or integrity.

Users assume responsibility for personal account use. Consequently, users may not disclose passwords or make available the district network or devices. Moreover, the possession or use of others’ passwords, personal identification numbers (PINs), private digital certificates, or other secure identification information is prohibited.

Physical theft, rearrangement, or damage to any district device or network equipment, facilities, or property is strictly prohibited, and will be reported to authorities. Users of a district-owned device must immediately report the loss, theft, or unauthorized access of the device to their building administrator and the IT Director.

Loud or disruptive behavior that hinders academic work in and around the computer labs is not permitted.

Users with personally-owned devices on the district network are expected to take reasonable precautions to ensure security. Individuals may be held responsible for misuse by others that occur on their devices. School District staff will scan the district network, and devices connected to it, to assist in identifying and protecting against security vulnerabilities. Devices may be disconnected from the district network until security issues have been resolved.

Users are not permitted to register external domain names or any domain that reference systems on the district network.
Users shall not connect any secondary device, including bridges, routers, or wireless access points, to the district network.

**Electronic Communication**

Students and staff are expected to follow the same standards of behavior in the use of electronic communication as in written and oral communication and to follow all appropriate standards of behavior and conduct rules. Therefore, electronic communication must be neither obscene nor constitute harassment, must not misrepresent the identity of the sender, and should not be used to send chain letters or broadcast indiscriminately to large numbers of individuals.

Users must keep personal information safe and private. Personal information such as age, home address, telephone number, social security number, and banking information should not be shared online. Users should never respond to email, click on links within email, or open attachments in emails unless 100% sure of the validity. Even then, users should never share personal information by clicking on a link from within an email or web site.

**Use of Social Media**

The school district supports relationships that develop within our school community’s classrooms and offices, and on our athletic fields. These types of relationships are based on academic grounds and are a natural part of most students’ elementary, middle and high school experiences. There are several educational benefits that these types of relationships can bring to our students, and we encourage the interaction.

It is not appropriate, for students and faculty, or students and staff to engage in social media exchanges that are not related to academic work. For some sites, users must be at least 14 years of age to legally connect. In any case, the practice of faculty and staff “Friending” students or accepting “Friend requests” from students, or otherwise sharing social media content, not directly related to academic work, is not endorsed by the SSD. In the interest of protecting the students, faculty and staff from negative consequences that can and do arise as a result of social media exchanges, such exchanges are prohibited.

**Cyberbullying**

Cyberbullying will not be tolerated. Harassing, dissing, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying.

**Harassment**

Repeated and unwanted electronic communication may constitute harassment. In general, communication targeted at a specific individual with the intent to harass or threaten is a violation of district policy. Individuals should notify senders when email or other forms of communication are unwanted. If the sender continues to communicate after being notified, the incident should be reported to a school administrator. Users are encouraged to retain electronic copies of all correspondence.

**Discrimination**

As outlined in district handbooks, district network or devices will not be used to discriminate against any person on the basis of race, color, religion, sex, national origin, age, disability, veteran status, or sexual orientation.

**Obscenity**

Obscenity is illegal and not tolerated.

Obscenity generally includes, but is not limited to, sexually explicit or pornographic content, a sexually offensive word or combination of words, profanity, swearing, or an expression or content, including lewd images. Questions about obscenity should be directed to a school administrator.

**Copyright**

Users must respect copyrights. Federal copyright law prohibits the reproduction, distribution, public display or public performance of copyrighted materials without permission of the copyright owner, unless Fair Use or another exemption under copyright law applies.
Using the district network or devices to download or share any copyrighted material including images, music, movies, television shows or games without the permission of the copyright owner may result in access revocation, legal sanctions, or both. Peer to peer file sharing programs like BitTorrent can transmit files from your device to others in violation of copyright laws, with or without user knowledge. If such programs are discovered on a user’s device, the user will be held responsible for resulting copyright violations.

Data Retention
A data retention policy ensures the most efficient and effective operation of the district network. It ensures that student, faculty and staff accounts, and associated records such as email and electronic files, are not retained unnecessarily past a reasonable period of time following faculty/staff separation and student graduation or withdrawal. Accounts and data related to faculty and staff is therefore retained for one full calendar year from the time the faculty or staff member separates from the district. Student accounts and data are deleted one year post high school graduation or withdrawal.

Sensitive Data
Downloading, copying, transmitting confidential or sensitive data (files that contain student records, financial data, HR records or medical information) should never be done on devices other than those provided by the district, and only when required as a part of a user’s work-related responsibilities. These types of files should also never be copied to portable storage, emailed or stored in cloud services like Dropbox.

Password Management
The combination of user ID and password will identify and authenticate a user. As such, passwords must be constructed, used, and protected appropriately to ensure that a minimum level of security is met. Password construction, lifecycle and re-use parameters vary depending upon the system or application they are intended to protect. All passwords should conform to the guidelines outlined in the table below:

<table>
<thead>
<tr>
<th>Guideline</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Construction</td>
<td>✔ Passwords should not be based upon well-known or easily accessible information, including personal information or words that can be commonly found within a standard dictionary.</td>
</tr>
<tr>
<td></td>
<td>✔ All passwords must be a minimum of eight (8) characters and must include characters from the two (2) categories below.</td>
</tr>
<tr>
<td></td>
<td>• Uppercase letters (A through Z)</td>
</tr>
<tr>
<td></td>
<td>• Numbers (0 through 9)</td>
</tr>
<tr>
<td>Password Lifecycle</td>
<td>Although the policy will vary appropriately based upon the security level of each system, in all cases passwords should be changed at least once a calendar year.</td>
</tr>
<tr>
<td>Password Reuse</td>
<td>You cannot use the same password for consecutive changes</td>
</tr>
<tr>
<td>Password Protection</td>
<td>✔ Do not share your password with teachers, staff or friends.</td>
</tr>
<tr>
<td></td>
<td>✔ Passwords must not be transmitted electronically over the Internet or through email.</td>
</tr>
<tr>
<td></td>
<td>✔ Never write your passwords down on paper as a memory mechanism.</td>
</tr>
<tr>
<td></td>
<td>✔ As a best practice and where feasible, each system/application, that requires a password, should have a unique password.</td>
</tr>
<tr>
<td></td>
<td>✔ Immediately report any suspicion of stolen passwords or unauthorized use of your account to SSD IT staff.</td>
</tr>
</tbody>
</table>

Technology Services Provided by Salem School District

Devices
To the extent that it can, the SSD provides devices to support students in their learning and faculty/staff in their work.

District Network
The District maintains a wired and wireless infrastructure and appropriate security to provide users access to online resources.

Adopted 6/16/15
Internet Access
Students are provided access to the Internet once parental permission is given. Faculty and staff are provided access to the Internet to support work-related responsibilities.

While the benefits of the Internet are enormous, users need to be aware that the Internet provides access to material that some people may find offensive. The district does not guarantee that users will not encounter objectionable text, pictures, or references. The district uses web filtering, as required by the Children’s Internet Protection Act (CIPA), and therefore provides protection against well-defined inappropriate material. The SSD is aware that not all inappropriate information can be filtered and will make an effort to correct any known information filtering breaches without unduly inhibiting the educational use of age appropriate content by students, faculty and staff.

Services and Applications
The district provides users access to a number of online services and applications to support learning and work. Visit http://sau57.org/technologyresources/onlineservices for a listing of these applications and services.
SSD Technology Responsible Use Policy
CONSENT AND PERMISSIONS FORM

Parents/Guardians should read this Salem School District Technology Responsible Use Policy and discuss the technology use responsibilities with their children prior to signing. Please print, complete and sign this Consent and Permissions Form for each child, and return to your child’s teacher. Faculty and staff should sign and return to Human Resources.

Check all that apply:

_____ Student: I have read and I understand the Salem School District Technology Responsible Use Policy. I further acknowledge that I will comply with this policy and understand that any violation may result in my access privileges being revoked, school disciplinary action, and in some cases may constitute a criminal offense.

_____ Parent/Guardian: As the Parent or Guardian I have read and I understand the Salem School District Technology Responsible Use Policy. I acknowledge that my child will comply with these policies. I understand that my child will have access to the Internet and services provided through the SSD that are designed for educational purposes and that the SSD has taken reasonable precautions to prevent access to inappropriate material and to protect the privacy of my child’s information. However, I recognize that it is impossible to prevent access to all inappropriate materials nor guarantee no loss of information. I will therefore not hold the SSD responsible for materials viewed, acquired, or communicated on the Internet or private accounts accessed. I further understand that any violation of this policy may result in: my child’s access privileges being revoked, school disciplinary action, and in some cases may constitute a criminal offense.

_____ SSD Faculty/Staff: I have read and I understand the Salem School District Technology Responsible Use Policy. I further acknowledge that I will comply with this policy and understand that any violation my result in my loss of access privileges, and disciplinary action up to and including dismissal.

____________________________________________________________________________________

The Children’s Online Privacy Protection Act (COPPA) requires parental consent for students under age 13.

_____ I give permission for my child (under age 13) to use the Internet and associated online services, approved and provided through the SSD. Please visit http://sau57.org/technologyresources/onlineservices for a listing of services.

_____ I do not want my child to be issued access to the Internet and associated online services.

____________________________________________________________________________________

By signing below I understand that I am acknowledging my replies, as indicated with a check mark, to all applicable content on the SSD Technology Responsible Use Policy CONSENT AND PERMISSIONS FORM:

<table>
<thead>
<tr>
<th>Student Name: (print first &amp; last)</th>
<th>____________________________________________</th>
</tr>
</thead>
<tbody>
<tr>
<td>Student Signature:</td>
<td>____________________________________________</td>
</tr>
<tr>
<td>Expected High School Graduation Year</td>
<td>________</td>
</tr>
<tr>
<td>Date Signed(mm/dd/yyyy):</td>
<td>________________</td>
</tr>
</tbody>
</table>
Parent/Guardian Name: (please print first & last)  ________________________________

Parent/Guardian Signature:  ________________________________

Date Signed (mm/dd/yyyy):  __________

Faculty/Staff Name: (please print first & last)  ________________________________

Faculty/Staff Signature:  ________________________________

Date Signed (mm/dd/yyyy):  __________