ST. JOHNS UNIFIED SCHOOL DISTRICT

1. ACCEPTABLE USE POLICY

For Student/Staff Use of Computers, Networks, and Internet Resources
2014 - 2015

Introduction

St. Johns Unified School District considers computers to be worthwhile tools for education and encourages the use of computer related technology in the classroom to supplement the educational goals of the District. Access to the Internet provides access to powerful educational resources which allow students to find information on networks anywhere in the world.

Just as the school has rules for acceptable behavior there are correct actions and rules that direct the use of information networks. If these guidelines are not followed you will lose your **privileges** to access the World Wide Web and to use District technology.

When a students or staff member in the District accesses computers, networks, and educational technology owned or operated by the District, he or she assumes certain responsibilities and obligations. All access of this type is subject to school policies and to local, state and federal laws. The St. Johns Unified School District expects that students and staff use of computers provided by this District will be ethical, for educational pursuits, and will reflect academic honesty. Students and staff are expected to demonstrate respect for intellectual property, system security and privacy of others.

Obligations & Expectations

As a student or staff member in the St. Johns Unified School District you are expected to make appropriate use of the computer resources provided by the District. The obligations that you assume and agree to by signing this agreement are:

- To use computers only for authorized purposes
- To be responsible for ALL activities on your assigned account. Do not share your account with anyone or leave the account open or unattended
- Report all potential security problems to a school administrator
- Access only files and data which are your own, which are publicly available or to which you have been given access
- Maintain the privacy of your password (do not reveal it to others)
- Never post a picture of a student without signed parental or guardian authorization

- Use only legal versions of copyrighted software which have been purchased by the District
- Be responsible for making a back-up of any personal files/documents that are critical to your use
- Be responsible for deleting unused files that are taking up unnecessary space on the District servers
- Make good use of limited network bandwidth by not downloading large files (especially videos, movies, music, games or other programs)

Inappropriate Use

It is the policy of St. Johns Unified School District to:

a) Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail or other forms of direct electronic communications
b) Prevent unauthorized access and other unlawful online activity
c) Prevent unauthorized online disclosure, use or dissemination of personal identification information of minors
d) Comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)]

Additional actions which are considered inappropriate use of District technology include, but are not limited to:

- Intentionally disrupting the network or crashing the network and connected systems
- Attempting to circumvent or sabotage system security measures
- Using computer programs to decode passwords or to access controlled information
- Using another person's data or files without permission
- Using another person's password or revealing your password to another student
- Engaging in any activity that might be harmful to systems, the network or any information stored thereon, such as damaging files or disrupting service
- Impersonating another user or acting in ANY anonymous fashion
- Downloading **ANY** programs without the Technology Director's approval
- Vandalizing or modifying hardware or software components in ANY way
- Copying files, data or programs from the Internet without permission
- Stealing data, equipment or intellectual property (such as downloading illegal music files or sharing music files, which is illegal)
- Bringing equipment from home and plugging it into the network without permission from, and a virus check by the Technology Department

- Attempting to gain access to or download from any site on the Internet which publishes material that is defamatory or pornographic in nature or which may incite racial hatred
- Obtaining unauthorized access to the District's wireless network

Student Safety

Education, Supervision and Monitoring

It shall be the responsibility of all members of the St. Johns Unified School District staff to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act and the Protecting Children in the 21st Century Act.

Procedures to prevent access to inappropriate material and for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Technology Director or designated representatives.

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet (or other forms of electronic communications) access to inappropriate information.

Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Designated representatives from each school will provide age-appropriate training for students who use the District's Internet facilities. Training shall include but is not limited to the following:

Safety on the Internet

- Guard your identifying information (name, sex, age, address, school, teams).
- It only takes a little information for a predator to identify you.
- Always remember, responsible adults do not pursue relationships with kids and teens.
- Make your username generic and anonymous.
- Make your online profile generic and anonymous.
- Know how to exit an inappropriate website.
- Attachments in e-mails from strangers can contain viruses and worms.

- Pictures are great to hand to a friend, but it's not cool to send them to an Internet 'friend.'
- Posting your picture on the Internet gives hackers the chance to doctor your picture and make fun of you to everyone on the World Wide Web.
- Chat room 'friends' are not always who they say they are.
- Know the rules about Intellectual Property. Do not illegally download music and movies.

Appropriate Behavior While Online - Including Interacting With Other Individuals on Social Networking Websites and in Chat Rooms

- Be careful what you write about others. Assume that anyone about whom you are writing will read your comments or receive them by some circuitous route
- Be truthful. Do not pretend to be someone or something that you are not
- Avoid offensive language, especially comments that might be construed as racist or sexist
- Remember that the law still applies in cyberspace. Do not commit illegal acts online, such as libeling or slandering others, and do not joke about committing illegal acts
- Be careful with humor and sarcasm. One person’s humorous comment can be another person’s boorish or degrading remark
- Generally speaking, avoid putting words into full capitals. Online, all-caps are considered SHOUTING
- Never send online chain letters
- Some e-mail programs allow one to place signatures containing text and graphics at the ends of mailings. Remember that elaborate materials take up valuable transmission time and do not overdo these signatures
- Do not send e-mail to people who might have no interest in it. In particular, avoid automatically copying e-mail to large numbers of people
- Avoid chastising others for their online typos. To err is human. To forgive is good cybercitizenship

Cyberbullying Awareness

Cyberbullying is the use of cell phones, instant messaging, e-mail, chat rooms or social networking sites such as Facebook and Twitter to harass, threaten or intimidate someone.

Cyberbullying can include such acts as making threats, sending provocative insults or racial or ethnic slurs, gay bashing, attempting to infect the victim's computer with a virus and flooding an e-mail inbox with messages.

If you are a victim, you can deal with cyberbullying to some extent by limiting computer connection time, not responding to threatening or defamatory messages and never opening e-mail messages from sources you do not recognize or from known sources of unwanted communications. Report cyberbullying to a District teacher or administrator.

Consequences of Violations

Consequences of violations include, but are not limited to:

- Suspension of network access
- Revocation of network access
- Suspension of computer access
- Revocation of computer access
- School suspension
- School expulsion
- Legal action and prosecution by the authorities

NOTE: **Students will be held accountable for completing assignments that require the use of computers even if their in-school computer access privileges are suspended or revoked.**

Be advised that it is a **federal offense (Felony)** to break into any security systems. Financial and legal consequences of such actions are the responsibility of the user (student, volunteer, staff) and the student's parent or guardian.

Tampering with computer security systems and/or applications and/or documents and/or equipment will be considered vandalism, destruction, and defacement of school property. Vandalism will result in cancellation of privileges, disciplinary action, and restitution for costs associated with hardware, software and system restoring. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, hardware, software or the network.

The System Administrator along with the school Principal may at any time suspend or revoke a user's privileges for any actions in violation of the guidelines above.

Privacy and Administrator's Access to User Files

St. Johns Unified School District is a public entity, therefore, all records (excluding those specified by law), whether in electronic or hardcopy form, are subject to the Freedom of Information Act and open to public inspection. **Network storage areas are subject to inspection.** Network administrators may review communications (emails, attachments, files) to maintain integrity system-wide and ensure that users are using the system in a responsible, acceptable manner. Users should NOT assume that their uses of the network are private. The district reserves the right to monitor network activity in any form that it sees fit to maintain system integrity, and to copy, examine and delete any files or information on the network that may suggest that a student/staff member is using school computers systems inappropriately.

ST. JOHNS UNIFIED SCHOOL DISTRICT ACCEPTABLE USE POLICY

AGREEMENT/SIGNATURE PAGE

For Parents and Guardians of District Students

My child and I have read the St. Johns Unified School District Acceptable Use Policy. We agree to abide by ALL the rules listed. We understand that violation of these rules may result in disciplinary action including, but not limited to, suspension or revocation of privileges, suspension or expulsion from school and criminal prosecution. We release the St. Johns School System and all other organizations related to the SJUSD Internet connection from any liability or damages that may result from the use of District computer systems. I understand that my Internet/Computer usage may be monitored for security reasons. In addition, we will accept **full** responsibility and liability for the results of any actions with regards to the use of the Network and the Internet. We release the school and related organizations from any liability relating to consequences from my use of the Internet.

Student Name (Please PRINT) _____

Signature of Student _____Grade _____ Date_____

Signature of Parent/Guardian _____ Date _____

Your student will not be allowed any access to district computers or the network without this signed agreement on file.

ST. JOHNS UNIFIED SCHOOL DISTRICT ACCEPTABLE USE POLICY

AGREEMENT/SIGNATURE PAGE

For Administrators, Teachers, Staff & Substitutes

I have read the St. Johns Unified School District Acceptable Use Policy. I agree to abide by ALL the rules listed. I understand that violation of these rules may result in disciplinary action including, but not limited to, suspension or revocation of privileges, limitations on technology usage and criminal prosecution. I release the St. Johns School System and all other organizations related to the SJUSD Internet connection from any liability or damages that may result from the use of District computer systems. In addition, I will accept **full** responsibility and liability for the results of any actions with regards to the use of the Network and the Internet. I understand that my Internet/Computer usage may be monitored for security reasons. I release the school and related organizations from any liability relating to consequences from my use of the Internet.

Employee Name (Please PRINT) _____

Signature of Employee _____ Date _____