**TROY SCHOOL DISTRICT**
**STUDENT TECHNOLOGY ACCEPTABLE USE POLICY**

**Philosophy**
Technology users (collectively, "Users" or, as applicable "Student Users" or "Employee Users") of the Troy School District (the "District"), at the discretion of the Superintendent or his/her designee, will be granted a login allowing access to the District's technology resources in order to promote personal academic growth, information gathering and communication. Technology resources include but are not limited to computing devices, servers, networking equipment and cabling, telecommunications and audio/video systems, software and access to the Internet and on-line services. The District's goal is to promote educational excellence through collaboration, creativity, critical thinking and communication opportunities made available by technology.

Other than as expressly set forth herein (i.e., specifically related to CIPA compliance), the District makes no specific promises about the technology resources provided by the District. For example, the District makes no commitments about the specific functions of the technology resources or their reliability, availability or ability to meet Student Users' needs. The technology resources are being provided "AS IS." The District will not be responsible for loss of data, service interruptions or for the accuracy or quality of information obtained through District technology resources. The District prohibits unlawful use of technology resources and in no way assumes responsibility for the actions of Student Users that could result in criminal or civil legal recourse.

**Student User Access**
A Student User's access to technology resources shall be considered a privilege with no entitlement or guarantee. Access may be revoked at any time at the discretion of the Superintendent or his/her designee. The District reserves the right to access all information generated by any Student User and review such content at any time it chooses and for any lawful purpose. There is no expectation of privacy with regard to the District's network or any data stored therein or which may be transmitted through the same. All Student Users, by their use of the District's technology, hereby consent to such access and review by the District. The District complies with all state and federal privacy laws.

**Student User Obligations**
All Student Users who access or use District technology resources are required to protect and care for any systems they are accessing or using, accept full responsibility for all actions performed under their user login, and know and obey District regulations and federal, state, and local laws and ordinances governing the use of technology. All violations will be addressed under the Student Code of Conduct. Student Users are expected to exercise good judgment and discretion in using technology resources and limit use to educational purposes.

Each Student User has the responsibility to use the District's technology resources appropriately by:

- Employing good digital citizenship;
- Using resources only for educational purposes during class time and/or to perform school-related work;
- Respecting all applicable law, including copyright laws and academic integrity;
- Not removing, modifying or destroying technology resources;
- Maintaining personal security by protecting passwords;
- Not attempting to gain unauthorized access to systems or trespassing in other Users' data files or directories;
- Complying with all the terms and conditions of the District's Acceptable Use Policy and Student Code of Conduct; and
- Reporting any violations or misuses of the Internet to an administrator.

The following behaviors are examples of prohibited behavior:

- Use of technology resources to send, receive, or display text, messages or images that could violate the District's non-discrimination and bullying (including cyber bullying) policies which could be considered threatening (i.e., placing a person in fear of imminent harm). Use that is obscene, pornographic, otherwise disruptive of or detracting from the educational mission of the school or that is potentially dangerous to District resources;
- Using another User's password, sharing a User's password with another person, modifying another User's account or invading, trespassing, hacking or otherwise gaining access to accounts, servers, filters, folders, files or other resources to which the User has not been granted specific rights;
- Harassing, insulting, threatening, bullying, stalking, intimidating, disrupting access, remotely controlling or shutting down systems, or other abusive or disruptive behavior;
- User disclosure of personal information about the User or others, including addresses, telephone numbers, credit card information, social security numbers, passwords or other confidential information via e-mail or the Internet;
- Installing, deleting, relocating, renaming, hiding, or modifying any hardware, software, games, applications ("Apps"), files, or network connections, entering system folders or the control panel or engaging in any activities intended to circumvent, avoid, or hide from District security measures or damage District technology;
- Use of technology resources for commercial or for-profit purposes, fundraising, distributing or forwarding chain letters, junk e-mail or advertising; and
- Unauthorized use of electronic devices unless approved by the classroom teacher, school administrator or designee.

**District Obligations Regarding Student Use**
In compliance with the Children's Internet Protection Act (CIPA), the District has installed filtering software to block or restrict access to Internet sites containing material that is (1) obscene; (2) child pornography; or (3) harmful to minors. The software evaluates websites based on criteria determined by the District. No software can keep up with the constant changes on the Internet. A Student User who accidentally connects to an inappropriate site must immediately disconnect from the site and notify an administrator, teacher or supervisor. Upon request, authorized staff may re-evaluate and unblock blocked sites to allow access.

**Internet Acceptable Use Policy**
The Internet is an important resource for students and will be used as an integrated part of the school curriculum. Parent/guardian permission must be granted to allow Students to use the internet in a supervised setting. If parents choose to opt out of allowing their child(ren) to use the internet in a supervised setting, they are hereby advised that their child(ren) will NOT be allowed to participate in school activities involving their direct use of the Internet via District technology resources, including, but not limited to, the following:

- Online activities research projects (math, science and language arts activities, etc.);
- Access to online District Media Center resources;
- Classroom activities in classrooms equipped with Smartboards when Internet-based resources are used;
- Web 2.0 activities; and
- Audio/Video conferencing activities.

To ensure that there is no confusion as to opt out status, technology and internet services may continue to be provided as described and governed herein unless a written opt out is received **annually** by the student's building principal.

Parents who choose to opt out of this Technology Use Policy will be required to attend a meeting with their child(ren)'s principal and/or other relevant school personnel to determine a course of action for times when their child(ren) will not be able to participate due to the parent's choice.

Students will be using a variety of online Web 2.0 websites, programs, and Apps as a resource to enhance their learning experience beyond the classroom. These tools will allow Students to better collaborate, create, research, store and work through our current curriculum. Although these tools are widely used by the educational community which supports their use in K-12 institutions, their Terms of Service state that due to Federal Law any users under the age of 13 must obtain parental permission to use their sites. Parental permission will be requested in such cases, either by District personnel or by the Terms of Service (or similar document) published by the website, program or App in question. Parents will be presumed by the District to have followed any and all required protocols for any internet services, including Web 2.0 services, if their child(ren) participate in said services. Parents who opt their child(ren) out of using any Apps or Web 2.0 websites or programs must observe the same opt out provisions set forth above for opting out of District Internet use.

All websites and tools have been and will continue to be thoroughly examined by experienced educators and are used commonly in education today, but new tools arise every day. The Children's Online Privacy Protection Act (COPPA) requires that websites obtain parental consent before collecting, using or storing "personally identifiable information" (PII) about children under 13 years of age. PII includes data such as first and last name, street address, telephone number or e-mail address. The District does not collect this type of information via the Internet. However, under COPPA, "collecting" includes not only a direct request, such as a registration form, but also enabling children to make PII available online. Examples of how a child could make PII available online include Web 2.0 websites, apps and e-mail. Internet safety lessons in our schools remind students that they should never reveal personal information online. Nonetheless, COPPA requires that web sites and services directed to children disclose their information collection, use and storage practices.

In order to honor our commitment to providing the best education possible, the District will provide Internet access to high-quality learning sites. We increasingly rely on educational resources on the Internet to provide a wide variety of activities that are rich in academic value that cannot be easily replaced. In an effort to increase our students' ability to work collaboratively on writing and research projects, we will be using a variety of free and approved Web 2.0 applications. Providing a 21st Century education that will prepare Students to be college and career ready is our highest priority, and the experience using the appropriate software for learning is an important part of that education.

**A list of all Troy School District approved Web 2.0 tools, sites and Apps is on the District webpage under Technology.** Here are several steps we take to protect Students:

- Students are appropriately supervised when using technology services at school.
- Students will continue to abide by the Acceptable Use Policy and the Student Code of Conduct.
- Students under the age of 13 cannot receive email communications from any non-approved addresses outside our district into our student email system. Our students use their school-provided email account to communicate with their teachers/peers and to safely sign up for logins on the approved Web 2.0 websites. For a list of the approved educational websites and Apps, please go to the website referenced above.
- Students are directed to age and subject appropriate sites without deceptive or excessive advertisements.
- Students will be assigned or instructed to login to certain websites allowed through the District Internet filter and approved by the District. These sites and/or Apps must abide by CIPA/COPPA policies.

**Disciplinary Action – Students**

Use of the Internet and District hardware and software is subject to all rules and regulations set forth in the Student Code of Conduct. Enforcement is the responsibility of the staff. Administration will review all cases referred for disciplinary action. In addition to disciplinary actions listed in the Student Code of Conduct, the administrator may exclude the student from access to the Internet or from using any and all computer equipment throughout the District.

| Level I Violations | Level II Violations | Level III Violations |
|---|---|---|
| Unauthorized use of electronic communication devices during school day | Harassment/Cyber bullying | Harassment/Cyber bullying (aggravated) |
| Unauthorized use of personal electronic communication devices during school day | Inappropriate Use of Technology Resources | Inappropriate Use of Technology Resources (aggravated) |
| | Stealing, Possession or Transfer of Property of Others (Value Under $100) | Stealing, Possession or Transfer of Property of Others (Value $100 or more) |
| | Vandalism (Value Under $100) | Vandalism (Value Over $100) |
| | Academic Misconduct | |

Questions regarding this AUP should be addressed to your student's building Principal.

*The Student and his/her Parent(s) or Guardian(s) understand and agree to all of the Obligations outlined in this Technology Acceptable Use Policy and further agree to indemnify and hold harmless Troy School District, its Board members, officers, and employees, and all organizations affiliated with Troy School District's Internet connection, for any and all claims of any nature arising from the Student's use of the Troy School District's computer hardware, software and/or Internet connection*.

Revised Dec 2019 (GD)