

Electronic Resources

Acceptable Use Procedures for Electronic Resources

The Acceptable Use Procedures 2022P are written to support the Electronic Resources Policy 2022 of the Auburn Board of Directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship represents more than technology literacy. Successful, technologically-fluent digital citizens live safely and civilly in an increasingly digital world. They recognize that information posted on the Internet is public and permanent and can have a long-term impact on an individuals' life and career. Expectations for student and staff behavior online are no different from face-to-face interactions.

Use of Personal Electronic Devices

In accordance with all Auburn School District policies and procedures, students and staff may use personal electronic devices (e.g. laptops, mobile devices and e-readers) to further the educational and research mission of the Auburn School District. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds. Staff using personal electronic devices for district purposes are required to document retention policies, if applicable.

Network

The Auburn School District network includes wired and wireless devices and peripheral equipment, files and storage, e-mail and Internet content (e.g. blogs, websites, collaboration software, social networking sites, wikis, etc.). The Auburn School District reserves the right to prioritize the use of, and access to, the network.

All use of the network must support education and research and be consistent with the mission of the Auburn School District.

The Auburn School District will not be responsible for any damages suffered by any user, including but not limited to, loss of data resulting from delays, non-deliveries, mis-deliveries or service interruptions caused by his/her own negligence or any other errors or omissions.

Acceptable network use by Auburn School District students and staff include:

- A. Creation of files, digital projects, videos, web pages and podcast using network resources in support of education and research;
- B. Participation in blogs, wikis, bulletin boards, social networking sites and groups and the creation of content for pod casts, e-mail and web pages that support education and research;
- C. The online publication of original educational material, curriculum related materials and student work. Sources outside the classroom or school must be cited appropriately;
- D. Staff use of the network for incidental personal use in accordance with all Auburn School District policies and procedures.

Unacceptable network use by Auburn School District students and staff includes but is not limited to:

- A. Personal gain, commercial solicitation and compensation of any kind;
- B. Actions that are unethical, illegal or result in liability or cost incurred by the Auburn School District;
- C. Support for or opposition to ballot measures, candidates and any other political activity;
- D. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools;
- E. Unauthorized access to other Auburn School District computers, networks and information systems;
- F. Cyberbullying, hate mail, defamation, harassment of any kind, discriminatory jokes and remarks;
- G. Information posted, sent or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
- H. Accessing, uploading, downloading, storage and distribution of obscene, pornographic or sexually explicit material;

- I. Physically altering parts or components of district technology devices without explicit prior approval of the Department of Technology.
- J. Downloading, copying or reproducing data, data sets, and/or data collections such as available in or derived from the core fiscal and student information systems, with the intent or result of removing from the Auburn School District premises said data without express prior approval of the superintendent or designee.

Internet Safety

Personal Information and Inappropriate Content:

- A. Students and staff should not reveal personal information, including a home address and phone number on web sites, blogs, podcasts, videos, social networking sites, wikis, e-mail or as content on any other electronic medium;
- B. Students and staff should not reveal personal information about another individual on any electronic medium without first obtaining permission;
- C. Student pictures or names can be published on any public class, school or Auburn School District website unless the parent or guardian has opted out; and
- D. If students or staff encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.

Internet Safety Instruction

All students will be educated about appropriate online behavior, including interacting with other individuals on social networking sites and chat rooms, and cyberbullying awareness and response.

- A. Age appropriate materials will be made available for use across grade levels.
- B. Training on online safety issues and materials implementation will be made available for administration, staff and families.

Filtering and Monitoring

Filtering software is used to block or filter access to visual depictions that are obscene and all child pornography in accordance with the Children's Internet Protection Act (CIPA). Other objectionable material could be filtered. The determination of what constitutes "other objectionable" material is a local decision.

- A. Filtering software is not 100 percent effective. While filters make it more difficult for objectionable material to be received or accessed, filters are not a solution in themselves. Every user must take responsibility for his/her use of the network and Internet and avoid objectionable sites;
- B. Any attempts to defeat or bypass the Auburn School District's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to Auburn School District browser settings and any other techniques designed to evade filtering or enable the publication of inappropriate content);
- C. E-mail inconsistent with the educational and research mission of the Auburn School District will be considered SPAM and blocked from entering Auburn School District e-mail boxes;
- D. The Auburn School District will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to Auburn School District devices;
- E. Staff members who supervise students, control electronic equipment or have occasion to observe student use of said equipment online, must make a reasonable effort to monitor the use of this equipment to assure that student use conforms to the mission and goals of the Auburn School District; and
- F. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct and assist effectively.
- G. The district will provide a procedure for staff members to request access to Internet websites blocked by the district's filtering software. The district will provide protocols for students, through the appropriate school channels, to request access to Internet web sites blocked by the district's filtering software. The requirements of the Children's Internet Protection Act (CIPA) will be considered in evaluation of the request. The district will provide an appeal process for requests that are denied.

Copyright

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. However, the duplication and distribution of materials for educational purposes is permitted when such duplication and distribution falls within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and content is cited appropriately.

Ownership of Work

All work completed by employees as part of their employment will be considered property of the Auburn School District. The Auburn School District will own any and all rights to such work including any and all derivative works, unless there is a written agreement to the contrary.

All work completed by students as part of the regular instructional program is owned by the student as soon as it is created, unless such work is created while the student is acting as an employee of the Auburn School District or unless such work has been paid for under a written agreement with the Auburn School District. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school. If under an agreement with the Auburn School District, the work will be considered the property of the Auburn School District.

Network Security and Privacy

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account for authorized Auburn School District purposes. Students and staff are responsible for all activity on their account and must not share their account password.

The following procedures are designed to safeguard network user accounts:

- A. Change passwords according to Auburn School District policy;
- B. Do not use another user's account;
- C. Do not insert passwords into e-mail or other communications;
- D. If you write down your user account password, keep it in a secure location;
- E. Do not store passwords in a file without encryption;
- F. Do not use the "remember password" feature of Internet browsers; and
- G. Lock the screen or log off if leaving the computer.

Student Data is Confidential

Auburn School District staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

No Expectation of Privacy

The Auburn School District provides the network system, e-mail and Internet access as a tool for education and research in support of the Auburn School District's mission. The Auburn School District reserves the right to monitor, inspect, copy, review and store without prior notice information about the content and usage of:

- A. The network;
- B. User files and disk space utilization;
- C. User applications and bandwidth utilization;
- D. User document files, folders and electronic communications;
- E. E-mail;
- F. Internet access; and
- G. Any and all information transmitted or received in connection with network (e.g. audio, video, multimedia, e-mail).

No student or staff user should have any expectation of privacy when using the Auburn School District's network. The Auburn School District reserves the right to disclose any electronic content to law enforcement officials or third parties as appropriate. All documents are subject to the public records disclosure laws of the State of Washington.

Archive and Backup

Backup is made of all Auburn School District e-mail correspondence for purposes of public disclosure and disaster recovery. Barring power outage or intermittent technical issues, staff and student files are backed up on Auburn School District servers regularly.

Disciplinary Action

All users of the Auburn School District's electronic resources are required to comply with the Auburn School District's policies and procedures. Violation of any of the conditions of use explained in the Auburn School District's Electronic Resources policy or procedures could be cause for disciplinary action, suspension or expulsion from school and suspension or revocation of network and computer access privileges.

Social Media and Electronic Communication

The Auburn School District understands the importance of staff, students and parents engaging, collaborating, learning and sharing in digital environments. The district is committed to effectively using a range of communication strategies and techniques to ensure the public, stakeholders, and staff are fully engaged and informed.

Staff have the following obligations and requirements when using social media tools:

- 1) All official Auburn School District presences on social media sites or services are considered an extension of the District's information networks and are governed by the Acceptable Use Procedures. This includes policies regarding personal use of District resources and policies regarding staff and student interaction.
- 2) Staff that use social media are responsible for complying with applicable federal, state, and county laws, regulations and policies. This includes adherence to established laws and policies regarding copyright, records retention, privacy laws (FERPA) and information security policies established by Auburn School District.
- 3) School social media accounts must be created using an official district email account.
- 4) Employees representing Auburn School District via social media outlets must conduct themselves at all times as representatives of the Auburn School District. Employees who fail to conduct themselves in an appropriate manner shall be subject to disciplinary action.
- 5) Violation of these standards may result in a request for the removal of staff/program pages from social media outlets.
- 6) District media sites, web pages and/or social media should promote learning/instruction, curriculum, school activities and/or information about the Auburn School District.
- 7) Auburn School District directory data are to be used when posting student photos, work, links, and information. Please consult your building principal/department supervisor and/or building secretary if you are not familiar with directory data releases and the accompanying procedures.
- 8) Staff should maintain a separation between professional and personal social media or electronic communication including text messaging
- 9) District presence on any social media site, including school related accounts, such as clubs, teams, field trips, course, or other sites associated with the district or a district school is authorized and monitored by the building principal or department supervisor.

Non-District Provided Social Media Sites Require Authorization Before Use

- 1) Staff use of Non-District Provided Social Media Sites is requested through the building principal/department supervisor. (ie Facebook; Twitter; YouTube Channel)
- 2) **Non-District Provided Social Media Site Use Authorization Form and Guidelines** are available on the Technology Department webpage.
- 3) When building principal/department supervisor approves (Non-District Provided) social media site use, principal or designee will inform the Communications Department before activating the site.