

PROCEDURE – STUDENT ELECTRONIC RESOURCES AND DIGITAL CITIZENSHIP 2022P

I. PURPOSE

These procedures are written to support the Electronic Resources and Internet Safety Policy of the Board of directors and to promote positive and effective digital citizenship among students and staff. Digital citizenship includes the norms of appropriate, responsible, and healthy behavior related to current technology use.

Successful, technologically-fluent digital citizens recognize and value the rights, responsibilities, and opportunities of living, learning, and working in an interconnected digital world. They recognize that information posted on the Internet can have a long-term impact on an individual's life and career. They cultivate and manage their digital identity and reputation and are aware of the permanence of their actions in the digital world. Expectations for student and staff behavior online are no different from face-to-face interactions.

II. USE OF ELECTRONIC DEVICES

Personally Owned Devices

In accordance with all District policies and procedures, students may use personal electronic devices (e.g. laptops, mobile devices, and e-readers) to further the educational and research mission of the District. School staff will retain the final authority in deciding when and how students may use personal electronic devices on school grounds and during the school day. Absent a specific and articulated need (e.g. assistive technology), students do not have an absolute right to possess or use personal electronic devices at school.

District Provided Devices

Students are furnished technology equipment by the District, based on their grade level and the appropriate level of access to these tools. In general, these are the extent to which technology equipment should be used for District-related school. School staff will retain the authority to decide when and how students may use District electronic devices on school grounds and during the school day.

III. NETWORK

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

All use of the network, as well as any materials stored, transmitted, or published on the system, must be in conformity to state and federal law-including FERPA and CIPA, network provider policies and District policy. All use of the network must support education and research and be consistent with the mission of the District.

From time to time, the District may determine whether specific uses of the network are consistent with the regulations stated in this procedure. Under prescribed circumstances, non-student or staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the District.

For security and administrative purposes, the District reserves the right for authorized personnel to review system use and file content including, without limitation, the contents of District-provided personal and shared file storage, web browsing history on a District device and/or the District network, and District email. Email is archived as per Public Disclosure Laws.

Acceptable network use by District students include:

- A. Creation of files, digital projects, videos, web pages, and podcasts using network resources in support of education and research;
- B. Participation in blogs, wikis, bulletin Boards, social networking sites and groups as permitted under District filtering limitations, and the creation of content for podcasts, e-mail, and webpages that support education and research;
- C. With parental permission, the online publication of original educational material, curriculum-related materials, and student work. Sources outside the classroom or school must be cited appropriately;
- D. Connection of personal wireless electronic devices to the filtered District guest network to support learning. Connection of any personal electronic device is subject to all procedures in this document and District policy.

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

- A. Personal gain, commercial solicitation, and compensation of any kind;
- B. Actions that result in liability or cost incurred by the District;
- C. Downloading, installing and use of games, audio files, video files, games, or other applications (including shareware or freeware) without permission.
- D. Support for or opposition to ballot measures, candidates, and any other political activity;
- E. Hacking, cracking, vandalizing, the introduction of malware, including viruses, worms, Trojan horses, time bombs, and changes to hardware, software, and monitoring tools;
- F. Making use of the electronic resources in a manner that serves to disrupt the operation of the system by others, including modifying, abusing, or destroying system hardware, software, or other components.
- G. Attempting to gain or achieving unauthorized access to other District computers, networks, and information systems;

- H. Action constituting or contributing to harassment, intimidation, or bullying, including cyberbullying, hate mail, defamation, discriminatory jokes, and remarks. This may also include the manufacture, distribution, or possession of inappropriate digital images;
- I. Information posted, sent, or stored online that could endanger others (e.g., bomb construction, drug manufacturing);
- J. Accessing, uploading, downloading, storage and distribution of obscene, pornographic, or sexually explicit material;
- K. Attaching unauthorized devices to the District network. Any such device will be confiscated, and additional disciplinary action may be taken; or
- L. Any unlawful use of the District network, including but not limited to stalking, blackmail, violation of copyright laws, and fraud.

The 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. The District will not be responsible for unauthorized financial obligations resulting from the use of, or access to, the District's computer network or the Internet.

IV. DIGITAL CITIZENSHIP INSTRUCTION

Lessons on digital citizenship, online safety issues, and cyberbullying awareness/response will be provided to all students and updated regularly. Students will be educated regarding appropriate digital citizenship according to 2023 – Digital Citizenship and Media Literacy.

Personal Information and Inappropriate Content:

- A. Students 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 should not reveal personal information about another individual on any electronic medium without first obtaining permission;
- C. No student pictures or names can be published on any public class, school, or District website unless the appropriate permission has been obtained according to District policy;
- D. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority;
- E. No user may use, disclose, or disseminate personally identifiable information of a minor without explicit parent/guardian permission;

- F. Students should be aware of the persistence of their digital information, including images and social media activity, which may remain on the Internet indefinitely.

V. MEDIA LITERACY

Media literacy is the ability to access, analyze, evaluate, create and act using a variety of forms of communication. Media literacy includes the ability to understand how and why media messages and images are constructed and for what purposes they are used.

NTPS will support students in developing the habits of inquiry and skills of expression that they need to be critical thinkers, effective communicators, and media literate citizens in today's world. See 2023 – Digital Citizenship and Media Literacy for additional guidance.

VI. SOCIAL MEDIA AND STUDENT EMAIL

Online communication is critical to students' learning 21st-century-skills. Internet and social media tools offer an authentic, real-world vehicle for student expression. The District holds students using these tools to the same responsible use, terms of agreement, and expectations, and students must follow all established internet safety guidelines. When these tools are used by students with District provided devices, while on District property or remotely, the District reserves the right to monitor appropriate behavior and adherence to instructional guidelines. The District may take disciplinary actions as appropriate when internet safety guidelines are not followed.

The District provides students with free email service for educational purposes only. These accounts are offered to students and managed by the District to provide consistent and reliable communication with their teachers. Use of these email accounts is subject to the same conditions and restrictions applicable to use of the District's network.

The District maintains the right to restrict or withdraw account access should there be reason to believe that the account has been misused or that the individual has violated the District's policies or the responsible use guidelines. Violation of District policy or these guidelines by staff, students and/or guests may result in disciplinary action as well as revocation of network and computer access privileges.

VII. 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 District's Internet filter or conceal Internet activity are prohibited (e.g., proxies, https, special ports, modifications to 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 District will be considered SPAM and blocked from entering District e-mail boxes;
- D. The 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 District devices.;
- E. The District may monitor student use of the District network, including when accessed on students' personal electronic devices and devices provided by the District, such as laptops, Chromebooks, and tablets;
- G. The District may block or delete any malicious content detected.

VIII. 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.

Personally licensed video streaming services (e.g. Netflix, Hulu, Amazon Video, Disney+ etc.) shall be blocked by District filtering software to prevent student, staff, and the District from violating the end user agreements of the platforms prohibiting non-personal and/or public viewing.

XI. OWNERSHIP OF WORK

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 school system or unless such work has been paid for under a written agreement with the school system. If under an agreement with the District, the work will be considered the property of the District. Staff members must obtain a student's permission prior to distributing his/her work to parties outside the school.

XII. NETWORK SECURITY

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 District purposes. No user will share their District account password. Students are responsible for all activity on their account and will:

- A. Lock the screen or log off if leaving the computer;
- B. Secure passwords according to District policy/rules;
- C. Not use another user's account;
- D. Keep account passwords confidential and safe, including not inserting passwords into e-mail or other communications;
- E. Not storing passwords in a file without encryption; and
- F. Not using the "remember password" feature of internet browsers.

XII. NO EXPECTATION OF PRIVACY

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

- A. The District network, regardless of how accessed;
- 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 and e-mail use.

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

XIII. ARCHIVE AND BACKUP

Backups are made of all District files and 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 District servers regularly. Refer to the District retention policy for specific records retention requirements.

XIV. ARTIFICIAL INTELLIGENCE

Artificial Intelligence is a rapidly advancing set of technologies for capturing data to detect patterns and automate decisions. Artificial Intelligence (AI) has become an increasingly important part of our lives, and it is essential for students to understand when and how to use it effectively and ethically. AI tools can enhance classroom learning, and their implementation should be guided with proper training, ethical considerations, and responsible oversight. When utilizing generative AI tools to create or support the creation of texts or creative works, students are expected to adhere to these guidelines, the Student AI Code of Conduct, and any additional guidance provided by their classroom teacher.

Purpose

The District will seek to maintain staff and student access to generative Artificial Intelligence tools for the following purposes:

- A. Ensuring all students have equitable access to leverage these technologies, regardless of what learning technology devices may be available to them.
- B. Providing all students with an opportunity to engage in current technologies in a learning environment, to better prepare them for the world they will live and work in.
- C. Extending the benefits of these tools to the workplace, where appropriate, to leverage efficiencies and productivity.

Appropriate Use

Student use of generative Artificial Intelligence technologies should be used to support and extend student learning. Student use of AI will be in accordance with the expectations outlined in Policy 2022, this document (2022P), and the AI Code of Conduct (2023A).

Inappropriate Use

In addition to those uses that violate this procedure the following are prohibited uses of Artificial Intelligence:

- A. Any use of Artificial Intelligence that does not align with expectations outlined by a classroom instructor or building administrator. It is ultimately the teacher's responsibility to determine the appropriate level of use of Artificial Intelligence in each classroom, and for each assignment or project.
- B. Use of Artificial Intelligence to complete an assignment in a way that represents the assignment as one's own work.
- C. Use of Artificial Intelligence to purposefully create misinformation or to misrepresent others for the purpose of harming or bullying groups or individuals.

D. Use of Artificial Intelligence with confidential student or staff personal information.

XV. DISCIPLINARY ACTION

All users of the District's electronic resources are required to comply with the District's policy and procedures and agree to abide by the provisions set forth in the District's user agreement as well as associated documents such as the AI Code of Conduct. Violation of any of the conditions of use explained in any of these documents could be cause for suspension or revocation of network, computer access, or other electronic resources privileges. Additionally, violations of these documents could result in disciplinary action, including suspension from school and/or civil or criminal actions, as warranted.

XVI. ACCESSIBILITY OF ELECTRONIC RESOURCES

In compliance with federal and state law, all District-sponsored programs, activities, meetings, and services will be accessible to individuals with disabilities, including persons with hearing, vision, and/or speech disabilities.

Adopted: December 11, 2018

NTPS Board of Directors

Amended: August 16, 2024

NTPS Cabinet