PROCEDURE – STAFF ELECTRONIC RESOURCES AND DIGITAL CITIZENSHIP 5022P

I. PURPOSE

These procedures are written to support the Electronic Resources 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 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. NETWORK USE

The district electronic "network" includes the wired and wireless network, telecommunication devices (two-way radios, smart phones, cellular phones, wired phones, long distance capabilities, etc), hardware, computers, tablets, software, and peripheral equipment, including, but not limited to handheld devices, files, storage, scanners, email, and Internet.

All use of the network must support education and research and be consistent with the mission of the district.

A. Users will be held strictly responsible for all activity that takes place on their accounts. System logins, passwords and accounts are to be used only by the authorized user of the account for the authorized purpose. Users may not share passwords or leave an open file or session unattended or unsupervised.
B. Users shall not seek information on, obtain copies of, or modify files, data, or passwords belonging to other users; misrepresent other users on the network; or attempt to gain unauthorized access to any part of the network.
C. The district reserves the right to examine all data created on, posted or stored on, or transmitted by the network.
D. Inappropriate content and activities on the network, such as cyberbullying, impersonating another, hate mail, defamation, harassment, or intimidation of any kind, are prohibited.
E. Hacking, cracking, vandalizing, the introduction of viruses, worms, Trojan horses, time bombs and changes to hardware, software and monitoring tools is prohibited.
F. Creating, posting, sending, or storing information on the network that could endanger others, such as bomb construction and drug manufacturing, is prohibited.
G. Sending, accessing, uploading, downloading, viewing, storage and distribution of obscene, pornographic, sexually explicit, or suggestive material is prohibited.
H. Users must not do anything that will damage the network, technology equipment or systems.
I. Users must not do anything that will disrupt the network or its operation.
J. The network constitutes public facilities and may not be used to support or oppose political candidates, ballot measures, personal gain, commercial solicitation, and compensation of any kind.

K. Users shall not attach any unauthorized devices of any kind to the district network. Any such device will be confiscated and additional disciplinary action may be taken.
L. Users shall not download or install of games, audio files, video files, games or other applications (including shareware or freeware) without permission or approval from Technology.

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.

III. INTERNET SAFETY AND DATA SECURITY

A. Staff and students should not reveal personal information, such as complete names, addresses and telephone numbers, about themselves or others on any electronic medium without permission
B. No staff member may disclose, use, or disseminate personally identifiable information about students, including photographs, to anyone other than staff with a legitimate educational purpose in the information. See Policy and Procedure 3600 and 3600P.
C. 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. Staff and students are responsible for all activity on their account and must not share their account password.
D. No student pictures or names may be published on any class, school, or district website unless the appropriate permission has been obtained according to district policy.
E. If students encounter dangerous or inappropriate information or messages, they should notify the appropriate school authority.
F. If any staff member suspects that personally identifiable information of staff, students, or guardians has been compromised, they should notify their supervisor immediately.

The following procedures are designed to safeguard network user accounts:

A. Change passwords according to 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.

IV. DIGITAL CITIZENSHIP INSTRUCTION

To prepare students for a digitally connected world and to comply with federal E-Rate requirements, all students will be educated about appropriate online behavior. Students will be taught to recognize and value the rights, responsibilities and opportunities of living, learning, and working in an interconnected digital world, and they engage in safe, legal, and ethical behaviors.

This includes interacting with other individuals on social networking websites, in chat rooms, and cyberbullying awareness and response.

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

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.

VI. SOCIAL MEDIA AND STUDENT EMAIL

Online communication is critical to students' learning 21st-century-skills. Social media, Internet tools such as blogs, wikis, social networks, podcasts, email, etc. offer an authentic, real-world vehicle for student expression. The district holds staff and students using these tools to the same responsible use, terms of agreement, and expectations, and staff and students must follow all established Internet safety guidelines. When these tools are used by staff or students with district resources, while on district property or while acting as a representative of the district, the district reserves the right to monitor appropriate behavior and adherence to instructional guidelines. Anything deemed to be inappropriate will be subject to deletion. The district may also take other disciplinary actions as appropriate. All social media accounts used on behalf of a school organization, school, department, or staff member, must be approved by Community Relations and Technology – with access given for monitoring and archival purposes.

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 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. STAFF SOCIAL MEDIA USAGE

A. Staff are prohibited from inappropriate online socializing with students or from engaging in any conduct on social networking Web sites that violates the law, district policies, or other generally recognized professional standards.

Employees whose conduct violates this policy may face discipline or termination, consistent with the district's policies, responsible use agreement and collective bargaining agreements, as applicable.

B. Staff are encouraged to use appropriate privacy settings to control access to their personal social media sites although there are limitations to privacy settings. Private communication published on the Internet can easily become public; social media sites can change their current default privacy setting\s and other functions. As a result, employees have an individualized responsibility to understand the rules of the social media site being utilized.
C. Staff should not "tag" photos of other district employees, district volunteers, district contractors or district vendors without the prior permission of the individuals being tagged.
D. Personal social media use, including off-hours use, has the potential to result in disruption at school and/or the workplace, and can be in violation of district policies and federal and/or state law.
E. The posting or disclosure of personally identifiable student information or confidential information via personal social media sites, in violation of these guidelines is prohibited.
F. Staff should not use the district's logo in any postings or post district material on any personal social media sites without the written permission of a district administrator.

VIII. STAFF USE OF NON-NTPS ELECTRONIC RESOURCES

Under Washington law, district staff are required to conduct themselves as role models for students at all times even when using non-NTPS networks and electronic information systems, such as personal computers and cell phones, e-mail accounts, websites and social networking sites and services. Staff should expect that any record created will be subject to review and possible disclosure under the Public Records Act (Chapter 42.56 RCW) if the staff member was conducting district or school business, including any communication with students. Staff has a legal obligation to report any reasonable suspicion of child abuse or neglect (per state law and Board Policy 3421, Child Abuse, Neglect and Exploitation Prevention) or infraction of school rules (per district policies, state law and the professional code of conduct) that arise from communication with students using non-NTPS electronic resources. This applies, for example, to staff-student text messages and interactions on Facebook or other social networks.

To support compliance with the law and to protect students and staff, the district has partnered with multiple third-party web platforms for staff to maintain any job-related web presence. If staff wish to maintain a job-related presence on a third party, non-district standard electronic resource, it must be reviewed by district technology prior to use. Specifically, the web platform must ensure compliance with the Public Records Act by archiving the site's content and metadata and certifying that they are maintaining such an archive for producing records when requested by the district.

Additionally, staff using any third party electronic resource shall not disclose any personally identifiable information about students. Any staff-created forum for student interaction will be conducted in a group or page by membership or approval of invitation to join or "like" a page not accessible by the general public (i.e., protected by membership), but shall be accessible to the students' parent or guardian upon request. It is the district's expectation that the supervisor and parent and/or guardian are notified of the staff-created web-presence. Staff can request a list of district supported web platforms from Technology Support Services.

IX. CONFIDENTIALITY AND COPPA COMPLIANCE

Generally, district staff must maintain the confidentiality of student data in accordance with the Family Educational Rights and Privacy Act (FERPA).

In addition, North Thurston Public Schools (NTPS) provides our students with access to various third-party websites, applications and other online resources to support student learning (the "Online Resources"). These Online Resources include, G Suite, Canvas, Renaissance Place, Typing Club, Learn360, and other similar educational programs.

In order for our students to use these Online Resources, the third-party operators of these Online Resources may collect certain personally identifying information (e.g., the students first and last name, username, and district email address). Under the federal Children's Online Privacy Protection Act (COPPA), these third-party operators must notify parents/guardians and obtain parent/guardian consent before collecting personal information of students under the age of 13. However, COPPA allows education institutions like NTPS to consent to this collection on behalf of parents, as long as the use of the personal information collected is limited to an educational context and is not used for any other commercial purpose.

Any staff member wanting to use a third-party Online Resource with student information needs to verify with district technology support that it is COPPA compliant and approved for district use.

X. FILTERING AND MONITORING

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

A. Filtering software is not 100% effective. Every user must take responsibility for his/her use of the network and avoid objectionable sites.
B. Any attempts to defeat or bypass the district's filter or conceal activity are prohibited.
C. 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.
D. 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 district.
E. Staff must make a reasonable effort to become familiar with the Internet and to monitor, instruct, and assist effectively.

XI. PERSONAL DEVICES

By connecting a personal electronic device to the North Thurston Public Schools network or e-mail system, you acknowledge and agree that NTPS reserves the right to enforce any security measures deemed necessary. This includes, but is not limited to:

A. Monitoring your use of the district network and email transmissions.
B. Remotely deleting the contents of your personal electronic device if lost when connected to district email. This may include district and personal contacts, pictures, other media, etc. Lost devices not connected to the district's email server will have their access blocked immediately.
C. Enforcing the use of a password/pin to access the mobile device when connected to district email.
D. Restricting the use of web applications deemed a security risk or non-educational in nature when on the district wireless network.
E. Restricting access to the district's network, including email system, based upon evidence that you failed to abide by conditions outlined in this Responsible Use Policy and User Agreement, or any misconduct in violation of district policy/procedure, and any violation of state or federal law.

In addition, documents or records of a public agency, including electronic communications using the district's network, are public records under Washington state law. Using any personal electronic device or computer for school district business may result in a requirement that you submit your personal device for examination if a public records request is received concerning information that may be stored on your personal device.

In accordance with all district policies and procedures, students and the community may use personal electronic devices (e.g. laptops, mobile devices and e-readers) to further the educational goals of the district and support community use of facilities. NTPS staff will retain the final authority in deciding when and how students and the community may use personal electronic devices on school grounds and during the school day.

XII. COMPLIANCE WITH COPYRIGHT AND OTHER LAWS, POLICIES, AND PROCEDURES

A. All use of the network must be in conformity with state and federal laws, network provider policies, and district policies and procedures.
B. Users must obey all copyright laws and other laws governing intellectual property rights. Unauthorized downloads, copies, duplications, installation, use, storage, or distribution of copyrighted software or material is prohibited. (See Copyright Policy 2312).
C. Personally licensed video streaming services (e.g. Netflix, Hulu, Amazon Video, etc.) shall be blocked by district filtering software to prevent staff and the district from violating the end user agreements of the platforms prohibiting non-personal and/or public viewing.
D. Users are expected to read and comply with all district standards (NTPS Standards Manual), Policies 2192, 8400, 3600 and Procedures 2192P and 3600P.

XIII. OWNERSHIP OF WORK

All work completed by employees as part of their employment will be considered property of the district. The 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 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.

XIV. 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, including when accessed on students' personal electronic devices and on devices provided by the district, such as laptops, netbooks, and tablets;

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 or staff user should have any expectation of privacy when using the district's network. 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.

XV. ARCHIVE AND BACKUP

Back-up is made of all district e-mail correspondence, approved social media posts and comments, and websites changes 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.

XVI. ACCESSIBILITY OF ELECTRONIC RESOURCES

Federal law prohibits people, on the basis of disability (such as seeing and hearing impairments), from being excluded from participation in, being denied the benefits of, or otherwise being subjected to discrimination by the district. To ensure that individuals with disabilities have equal access to district programs, activities, and services, the content and functionality of websites associated with the district should be accessible. Such websites may include, but are not limited to, the district's homepage, teacher websites, district-operated social media pages, and online class lectures.

District staff with authority to create or modify website content or functionality associated with the district will take reasonable measures to ensure that such content or functionality is accessible to individuals with disabilities. Any such staff member with questions about how to comply with this requirement should consult with the districts website administrator.

XVII. DISCIPLINARY ACTION

All users of the district's electronic resources are required to comply with the district's policy and procedures. Violation of any of the conditions of use explained in the Electronic Resources policy or in these procedures could be cause for disciplinary action, including suspension or expulsion from school, suspension or revocation of network and computer access privileges, and other appropriate legal or criminal action, including restitution, if appropriate. Staff violations are subject to the above-mentioned disciplinary actions up to and including termination of employment.

Adopted: December 11, 2018 North Thurston Public Schools Board of Directors