

Employee Agreement for Acceptable Use of the District Electronic Communications System

The purpose of this document is to set forth the policies governing the use of all District technology resources by employees while on or near school property, in school vehicles and at school-sponsored activities on- or off-campus, as well as the use of all District technology resources *via* off-campus remote access.

Please read the following Acceptable Use Policy carefully, as you will be held accountable for any failure to comply with it. The District reserves the right to modify the terms and conditions of this document at any time. The latest version of this document is available online at <http://www.neisd.net/aup/index.html>.

Introduction

NEISD is pleased to offer employees access to District computers, District communications systems¹, the Internet and a wide array of other technology resources to further its educational mission. The District will hold ALL employees responsible for their use of technology, whether District-provided or personal, and they are expected to act in an appropriate manner in accordance with campus procedures, District policy and procedures, and legal requirements. This applies to the use of all District technology resources by employees while on or near school property, in school vehicles and at school-sponsored activities on- or off-campus, as well as the use of all District technology resources *via* off-campus remote access.

Using the Internet and Communications Systems

The District provides technology resources to employees to enhance their ability to accomplish their particular job duties. This may be in the form of conducting research, improving instruction to students, completing assigned duties, and communicating with other employees, students and community members. Just as in the physical workplace, the District requires that employees demonstrate proper and professional behavior when using any District computer networks, software or websites sanctioned or used by the District, and any personal technology used in the workplace. Access to the District's technology is a privilege, not a right. Employees must comply with all District standards set forth in this policy at all times in order to maintain the privilege of using its technology resources.

Employees are advised that any information stored on and/or sent through the District's technology resources is the property of the District. Accordingly, District network administrators and/or other appropriate personnel may at any time engage in periodic reviews and searches of stored files and communications stored on District technology resources to maintain system integrity and ensure that employees are complying with this policy and using technology in a professional and appropriate manner. Employees do not have a reasonable expectation of privacy over any information stored on District technology.

Although the District strives to ensure that any Internet access avoids any inappropriate material, employees should be aware that some material accessible on the Internet may contain information that is inaccurate, profane, sexually oriented, defamatory and potentially offensive to some. The District does not condone, and will not tolerate, any employee accessing, or attempting to access, such material, and the District remains deeply committed to safe Internet use. The District takes steps to minimize

¹ "Communication systems" as used throughout this policy include educational-related communications between and among employees and students of the District by e-mail, web sites, cell phones, pagers, text messaging, instant messaging, blogging, podcasting, listservs, and/or other emerging technologies.

employees' opportunities to do so, including the implementation of extensive content-filtering software. This software is not fail-safe, however, and it is possible that the software may miss some content. Employees who find that content-filtering software has failed to block inappropriate content shall report it to their supervisor immediately.

This policy is strictly enforced. Any employee who misuses any District technology outside its intended purpose, including attempting to circumvent its content-filtering software without proper approval from a supervisor and in connection with a work-related purpose, will be in violation of this policy, which may lead to disciplinary action, up to and including termination of employment.

Proper and Acceptable Use of All Technology Resources

The District requires employees to use all technology resources, including any websites or software they may wish to use in an instructional setting, in a manner consistent with the following rules. The District will hold employees responsible for any intentional misuse of its technology resources, or any other failure to comply with the rules in this policy. When using District technology systems outside the workplace, employees must still do so in compliance with the rules set forth in this policy.

All District technology resources, including but not limited to District computers, communications systems and the Internet, including any websites or software to be used in a classroom setting, must be used in support of the District's educational mission, the accomplishment of job duties, and in accordance with the rules set forth in this policy.

Activities that are permitted and encouraged include the following:

- The improvement of instruction, collaboration, and accomplishing the employee's particular job duties;
- Original creation and presentation of academic work;
- Research on topics being studied and presented in school lessons;
- Research for opportunities outside of school related to community service or further education;
- Reporting content of an inappropriate or harassing nature to their supervisor;

Employees, such as classroom teachers, coaches or campus administrators, who seek to use websites, software, or other technology with students for instructional purposes, must do so in accordance with this policy. Employees shall use their best professional judgment to ensure that any technology implemented for use with students meets the District's standards, is age-appropriate, and is free from inappropriate content. Failure to exercise sound professional judgment in implementing technology in the classroom, such as using a website containing inappropriate content, will be seen as a violation of this policy for which the District can hold the employee accountable, including potential disciplinary action.

Activities that are barred and subject to potential disciplinary action and loss of privileges include the following:

- Using technology for plagiarism or otherwise representing the work of others as the employee's own;
- Presenting any copyrighted, registered, or trademarked work as that of the employee, or using any such work in violation of any applicable state or federal laws, including any use that exceeds the "fair use" doctrine;
- Using obscene or profane language on any District technology resource, to include posting such language on any website or software used by the District;

- Engaging in harassing, insulting, ostracizing, intimidating, unprofessional, or any other online conduct which could be considered bullying while using any District technology resource, to include the use of any website or software used by the District;
- Searching, viewing, communicating, publishing, downloading, storing, or retrieving any inappropriate or offensive material, or any material that is not related to the permitted activities set forth above;
- Using a website or software program implemented by the District in a manner outside the scope of the use specified by the District, or in a manner outside the scope of its terms and conditions;
- Engaging in any conduct that damages or modifies, or is intended to damage or modify, any District equipment, network, stored computer file, or software, to include any conduct that results in a person's time to take any corrective action;
- Intentional or neglectful transmission or direct placement of computer viruses or other unauthorized programs onto District equipment, networks, stored computer files, or software;
- Attempting unauthorized access, or "hacking," of District computers or networks, or any attempts to bypass Internet content-filtering software used by the District;
- Using USB, bootable CD's, bootable DVD's, or other devices to alter the function of any District technology equipment, network or software;
- Sharing online any personal information of another employee or a student, including name, home address, or phone number that is not included as part of an employee's job responsibilities;
- Using any District technology for games, role-playing multi-user environments, gambling, junk mail, chain mail, jokes, political or fundraising activities;
- Using any District technology resources for any commercial and/or for-profit purpose, to include personal financial gain or fraud;
- Using personal technology that provides Internet access to students without written permission from immediate supervisor;
- Using any District technology resource to engage in any activity that violates any NEISD Board policy DH(LOCAL)-A , the Educator's Code of Ethics, campus rule, local, state, and/or federal law.

Employees shall immediately report any violations of this policy to their supervisor. If any employee has any question about whether any activity may be a violation of this policy, they should consult with their supervisor.

Personal Use

Employees may use District technology resources for limited personal use during their non-working hours. Such use must be in compliance with this policy, and cannot interfere in any way with the employee's ability to complete their job duties.

Privacy and Security

Employees shall use District technology resources responsibly and in a safe and secure manner. Employees shall not share their individual logins, passwords, or access to District technology with others except to appropriate District Network Technology Services personnel or with the approval of the employee's supervisor. Employees shall sign off or log off all District equipment, software, or Internet sites once they are done with their session in order to protect the integrity of their logins, passwords or access.

Consequences for Violations of this Policy

Employees shall be subject to disciplinary action as deemed appropriate by the Superintendent or designee for a violation of this policy, depending on the severity of the violation. Such consequences may include, but are not limited to, verbal or written counseling, reprimands, suspension or placement on administrative leave, and termination. In addition, an employee's privileges to use District technology resources may be restricted or revoked. The District may undertake appropriate investigations of any potential violation of this policy by an employee, and may take action based upon the preponderance of the evidence revealed by such investigation.

Employees who violate this policy may also be subject to potential violations of local, state, and federal law, depending on the conduct involved.

Limitation of Liability

The District makes no warranties of any kind, whether express or implied, for the technology resources it provides to employees. NEISD is not responsible for any damages that an employee may sustain, including those arising from non-delivery of information, erroneous delivery of information, service interruptions, unauthorized use by an employee, loss of data, and any potential exposure to inappropriate material from the Internet. Use of any information obtained through the Internet is at the employee's own risk, as the District makes no representations, and denies responsibility for, the accuracy or quality of the information. In exchange for being allowed to use District technology resources, employees hereby agree to indemnify and hold harmless NEISD, its trustees, other employees, and representatives from any and all claims for damages that arise from their own intentional or neglectful misuse of the District's technology resources.

Revised 11/10/11