Havre Public Schools Acceptable Use Policy

1. Overview

Havre Public Schools' intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Havre Public Schools' established culture of openness, trust and integrity. Havre Public Schools is committed to protecting its employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of Havre Public Schools. These systems are to be used for business purposes in serving the interests of the district, and of our students and staff in the course of normal operations.

Effective security is a team effort involving the participation and support of every Havre Public Schools employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2. Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at Havre Public Schools. These rules are in place to protect the employee and Havre Public Schools. Inappropriate use exposes Havre Public Schools to risks including virus attacks, compromise of network systems and services, and legal issues.

3. Scope

This policy applies to the use of information, electronic and computing devices, and network resources to conduct Havre Public Schools business or interact with internal networks and business systems, whether owned or leased by Havre Public Schools, the employee, or a third party. All employees, contractors, consultants, temporary, and other workers at Havre Public Schools and its subsidiaries are responsible for exercising good judgment regarding appropriate use of information, electronic devices, and network resources in accordance with Havre Public Schools' policies and standards, and local laws and regulation. Exceptions to this policy are documented in section 5.2

This policy applies to employees, contractors, consultants, temporaries, and other workers at Havre Public Schools, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by Havre Public Schools.

4. Policy

4.1 General Use and Ownership

4.1.1 Havre Public Schools' proprietary information stored on electronic and computing devices whether owned or leased by Havre Public Schools, the employee or a third party, remains the sole property of Havre Public Schools.

4.1.2 You have a responsibility to promptly report the theft, loss or unauthorized disclosure of Havre Public Schools proprietary information.

4.1.3 You may access, use or share Havre Public Schools proprietary information only to the extent it is authorized and necessary to fulfill your assigned job duties.

4.1.4 Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

4.1.5 For security and network maintenance purposes, authorized individuals within Havre Public Schools may monitor equipment, systems and network traffic at any time.

4.1.6 Havre Public Schools reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

4.2.1 All mobile and computing devices that connect to the internal network must comply with the *Acceptable Use Policy*.

4.2.2 System level and user level passwords must comply with the *Password Policy*. Providing access to another individual, either deliberately or through failure to secure its access, is prohibited.

4.2.3 It is the responsibility of the employee to ensure that screens are locked when your device is unattended, in order to ensure the safety of all data.

4.2.4 Postings by employees from a Havre Public Schools email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of Havre Public Schools, unless posting is in the course of business duties.

4.2.5 Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain malware.

4.3 Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of Havre Public Schools authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Havre Public Schools-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities that fall into the category of unacceptable use.

4.3.1 System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Havre Public Schools.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Havre Public Schools or the end user does not have an active license is strictly prohibited.
3. Accessing data, a server or an account for any purpose other than conducting Havre Public Schools business, even if you have authorized access, is prohibited.
4. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
5. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
6. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
7. Using a Havre Public Schools computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
8. Making fraudulent offers of products, items, or services originating from any Havre Public Schools account.
9. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to HPS Tech Department is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
16. Providing information about, or lists of, Havre Public Schools employees to parties outside Havre Public Schools.

4.3.2 Email and Communication Activities

When using company resources to access and use the Internet, users must realize they represent the school district. Whenever employees state an affiliation to the district, they must also clearly indicate that "the opinions expressed are my own and not necessarily those of the school district". Questions may be addressed to the Personnel Department.

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within the Havre Public Schools networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Havre Public Schools or connected via Havre Public Schools' network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

4.3.3 Blogging and Social Media

1. Blogging by employees, whether using Havre Public Schools property and systems or personal computer systems accessing district networks, is also subject to the terms and restrictions set forth in this policy. Limited and occasional use of Havre Public Schools systems to engage in blogging is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate Havre Public Schools' policy, is not detrimental to Havre Public Schools' best interests, and does not interfere with an employee's regular work duties. Blogging from Havre Public Schools systems is also subject to monitoring.

2. Employees are prohibited from revealing any confidential or proprietary information when engaged in blogging.

3. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by Havre Public Schools whether using Havre Public Schools property and systems or personal computer systems accessing district networks.

4. Employees may also not attribute personal statements, opinions or beliefs to Havre Public Schools when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of Havre Public Schools. Employees assume all risk associated with blogging.

5. Policy Compliance

5.1 Compliance Measurement

The HPS School Board of Trustees will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner. The Superintendent or his designee shall have the final say in the execution of this process.

5.2 Exceptions

The Superintendent must approve any exception to the policy in advance.

5.3:Non-Compliance

Any violation of this policy, or negligent act resulting in a violation of this policy, is subject to discipline in accordance with District policy and applicable collective bargaining agreement. The School District reserves the right to seek remedies available under the law to recover financial losses to the School District resulting from employee negligence or intentional acts covered by this policy.

6. Related Standards, Policies and Processes

- Password Policy

7. Revision History

Date of Change	Responsible	Summary of Change
November 2016	HPS Tech Committee	Created/Edited
April, 2017	Mr. Mueller	Edited Language