SCHOOL TOWN OF HIGHLAND AUP

Acceptable Use of Technology

Purpose: To establish the foundation for technology literacy for the students and employees of the School Town of Highland.

By providing access to technology, the district intends to promote educational excellence in schools by facilitating resource sharing, innovation, communication and learning and by allowing access to resources unavailable through traditional means.

The availability of Internet access provides a unique educational opportunity for students and staff to contribute to the district's presence on the worldwide web. This medium of communication provides an opportunity to share accurate information with the community, the state and the world about the district's curriculum and instruction, school authorized activities and other related information. The district provided this instruction resource as an educational tool for staff and the technology acceptable use policy will govern it uses. The failure to follow this policy may result in the loss of privileges or other disciplinary measures as outlined in

The School Town of Highland has taken precautions to restrict access to inappropriate materials on the Internet. However, on a global network it is impossible to control all materials and a persistent user may discover inappropriate information. The school district believes that the valuable information and interaction available on this worldwide network far outweigh the possibility that users may procure materials that are not consistent with educational goals of the district. Users are responsible for reporting to the district's director of technology or his/her designee controversial or inappropriate websites they are able to access so the websites can be added to the district's filter.

In order to maintain access to the Internet, employees and students will abide by the rules and regulations for acceptable use outlined in administrative rule IJND-R. Unauthorized or inappropriate use of technology may include, but is not limited to: taking pictures or recording without permission, cheating, harassment or bullying, use during unauthorized times or use for unauthorized activities.

It is the purpose of this policy to establish basic rules for access/use of the Internet by students and employees in the School Town of Highland so that all use of this valuable resource is appropriate.

Personal use of social media

When staff members or students publish content, post pictures or maintain dialogue through Facebook or any other social networking tool, the professionalism, integrity and ethics in their role as an educator or student should never be compromised.

A Facebook fan page may not be used to replace a school or class website. A Facebook fan page is limited to extracurricular activities and clubs outside of the regular classroom. Staff members who want to use fan pages for student groups must have approval from the building administrator and from the district.

Inappropriate use of social media or electronic communication tools may result in disciplinary action up to and including dismissal.

Electronic mail (email) usage

The district's email system is made available to authorized users for educational and district operational purposes. All authorized users will receive instruction on proper use of the district email system.

The district prohibits the use of its email system for unprofessional and/or inappropriate purposes to include, but not be limited to, the following.

● Creating, transmitting or receiving emails containing any language or depictions that could reasonably be perceived by others as being offensive, threatening, obscene, sexual, racist or discriminatory

● Any use that violates local, state and/or federal laws or regulations

● Setting up or operating a commercial business

All electronic messages created, transmitted or received via the district's email system, including those created, transmitted or received for personal use, are the property of the district. The district reserves the right to archive, monitor and/or review all use of its email system and users should not have any expectation of privacy in any electronic message created, transmitted or received on the district's email system.

Handheld communication device usage

District-issued cell phones or other handheld communication devices are to be used only by the employee to whom the phone or communication device was issued and are to be used only for matters directly related to the employee's job responsibilities.

The district reserves the right to monitor and/or review all use of district- issued phones and communication devices and users should not have any expectation of privacy in any use of a district-issued phone or communication device.

Personal use of district research, information and communication resources

Limited personal use of district computers, the district network and the Internet and electronic research and communication resources is permitted to the extent that such use does not disrupt or interfere with the operation of the district and its instructional programs. Excessive personal use that may or does so disrupt or interfere is prohibited.

Third party access to systems and/or data

Within limited circumstances, the district sub-contracts specific work to be performed on behalf of the district in areas including, but not limited to, software development, system support, hardware acquisition and provisioning, and training. As part of these agreements, specific authority is granted to the sub- contracted third party to access the district's network and data, including student information and financial information. These agreements and authorizations of access to systems, networks or data are temporary in duration and bound by non-disclosure principles, confidentiality and time frames established within the agreement between the district and any third party. All local, state and federal statutes, laws or regulations regarding confidentiality of student information or financial information apply.

Sub-contracted work being performed on behalf of the district is limited to the specified parameters within the agreement. Upon completion of the agreed upon work, access to district systems or data is to be considered terminated. This termination of access will be accomplished either by manual action taken by the district technology department, or considered as the default access status of the third party following the completion of agreed upon work or tasks.

At no time will access to systems or data be continued beyond the completion of work or duration of specified time. Any physical or virtual access, either locally or remotely, to networks, systems or data must be approved by the district technology department or the superintendent. No other district entity holds the authority to grant access to any networks, systems or data. In circumstances where access is granted, the specific access is valid only for the duration of specifically agreed upon work and/or time frames. At the completion of agreed upon work,

access is considered terminated. Once access is considered terminated, new authorization of access must be granted by the district technology department or the superintendent prior to any new work, continuance of work or attempted access. Continuance of access authority is never automatic or to be assumed by any third party.

SCHOOL TOWN OF HIGHLAND

Acceptable Use Policy

This administrative rule governs the use of the district's computers, network, Internet and electronic research and communication resources by district employees, students and guest users and the use of personal electronic devices used on school property or during school-related events. It is intended to protect the integrity of district operations and instructional programs, as well as to outline the rights and responsibilities of district employees and guest users. These rules will be in effect at all times.

Scope

This administrative rule applies to the following persons/entities.

● all district employees including regular, part-time, temporary and contract employees

● all students enrolled in district schools

● all other authorized users of any of the district's technology resources, regardless of district affiliation or reason

for usage

● all district owned or operated technology resources or systems which are subscribed to and/or paid for by the district

● all personal electronic devices used on school property or during school- related events

Acceptable Use Agreements

At the beginning of each year, the district will review acceptable use policies through online registration and/or 1:1 parent meetings . At the elementary grades, the teacher or technology assistant will directly control all Internet access. In grades K-12, students will be required to read and sign the acceptable use contract. The contract must also be signed by the parent/legal guardian. Only those students with this signed contract on file will be allowed access to the

Internet. Employees must sign a similar contract. These contracts spell out guidelines for Internet use as well as consequences for violating the guidelines.

Confidential information

The district's research, information and communication resource systems have security measures in place; however, such measures do not guarantee total security. As a result, information generally considered to be personal or confidential should not be sent via the district's communication resources except through means deployed for that purpose or approved for that purpose. The district cannot assume responsibility for lost or stolen information sent or received via the district's communication resources.

General digital technologies usage and online access The following actions are prohibited.

● Knowingly loading or creating viruses

● Loading or attempting to load software or files onto a school computer without permission

● Loading or attempting to load software or files onto the district network without permission of the information

technology department

● Accessing or modifying data without authorization

● Modifying passwords without authorization

● Unauthorized access, including so-called "hacking" or other unlawful activities

● Unauthorized disclosure, use or dissemination of personal information regarding minors

Network and Internet usage

Access to the district network and Internet is made available to authorized users for educational and district operational purposes. All authorized users will receive instruction on proper use of the district's network and Internet system. Although students will be under teacher supervision while on the network, it is not possible to constantly monitor every individual student and what data they are accessing on the network. Some students might encounter information that is not of educational value. The district will not be liable for the users' inappropriate use of the district's electronic communication resources or violations of copyright restrictions, users'

mistakes or negligence, or costs incurred by users. The district will not be responsible for ensuring the accuracy or usability of any information found on the Internet.

The district prohibits the use of its network and the Internet to intentionally access, view, download, store, transmit or receive any information that contains material which is in violation of any district policy or administrative rule, or any local, state and/or federal laws or regulations.

Prohibited material includes, but is not limited to, the following.

• Obscenity or pornography

• Threats

• Material that is intended, or could reasonably be perceived, to be harassing or discriminatory

• Inappropriate use of material that is copyrighted or protected by trade secret • Material used to further any commercial business, product advertising, virus transmission or political activity

● Material that is potentially disruptive of the learning environment

The district reserves the right to monitor and/or review all uses of the district network and the Internet, and users should not have any expectation of privacy in any information accessed, viewed, downloaded, stored, transmitted or received.

Accessing inappropriate sites

The school district will use technology protection measures to the best of the district's ability to protect students from inappropriate access. Employee, student and visitor activities may be monitored by the district to detect unauthorized uses of the Internet and or access to inappropriate sites that have visual depictions that include obscenity, child pornography and other pornography or otherwise are violations of this administrative rule.

Reporting

District and school computer technicians as well as other district employees who are working with a computer and come across sexually explicit images of children must report this to local law enforcement. The report must include the name and address of the owner or person in possession of the computer.

Off-campus conduct

Students, parents/legal guardians, teachers and staff members should be aware that the district may take disciplinary actions for conduct initiated and/or created off-campus involving the inappropriate use of the Internet or web-based resources if such conduct poses a threat or substantially interferes with or disrupts the work and discipline of the schools, including discipline for student harassment and bullying.