STAFF NETWORK AND INTERNET ACCEPTABLE USE AND SAFETY POLICY AND AGREEMENT

Purpose

The purpose of this policy is to define the proper use of computers, computer networks, messaging systems, electronic mail (e-mail) systems, Internet, web, or online services by staff members in the School District.

Policy

It is the responsibility of each employee to ensure that this technology is used for proper educational purposes and in a manner that does not compromise the confidentiality of proprietary or other sensitive information.

Acceptable and Unacceptable Uses

The computers, computer network and messaging systems of the School District are intended primarily for educational uses and work-related communications only. The following are uses that are unacceptable under any circumstances:

- Staff members must always follow the prohibition against releasing education records or personally identifiable information as set forth in FERPA and other state and federal laws regarding student privacy.

- The transmission, posting, or downloading, of any language or images which are pornographic or of a graphic sexual nature.

- The transmission of jokes, pictures, or other materials which are obscene, lewd, vulgar, or disparaging of persons based on their race, color, gender, age, religion, national origin, or sexual orientation.

- The transmission of messages or any other content which would be perceived by a reasonable person to be harassing, demeaning, threatening, disruptive or inconsistent with the Board's policies concerning equal employment opportunity or sexual harassment.

- Uses that constitute defamation (libel or slander).

- Uses that violate copyright laws.

- Uses that attempt to gain unauthorized access to another computer system or to impair the operation of another computer system (for example, "hacking" and other related activities or the transmission of a computer virus or an excessively large e-mail attachment).

- Any commercial or profit-making activities.

- Any fundraising activities, unless specifically authorized by the appropriate authorized administrator.

- Any personal use or uses which are inconsistent with the educational goals and objectives of the School District.

Security and Integrity

Staff members shall not take any action which would compromise the security of any computer, network or messaging system. This would include the unauthorized release or sharing of passwords and the intentional disabling of any security features of the system.

Staff members shall not take any actions which may adversely affect the integrity, functionality, or reliability of any computer (for example, the installation of hardware or software not authorized by the System Administrator).

Staff members shall report to the I.T. Director or to a School District Administrator any actions by students or staff which would violate the security or integrity of any computer, network or messaging system whenever such actions become known to them in the normal course of their work duties. This shall not be construed as creating any liability for staff members for the computer-related misconduct of students.

On-Line Purchases

A staff member shall only use the network to make on-line purchases or payments for goods and services if the goods or services are being purchased by or on behalf of the School District. Such purchases or payments must still have the prior authorization of the building principal or Superintendent's designee.

Right of Access

The operational and security needs of the District's computer network, computers, telephones, voice mails, and other messaging systems require that full access be available at all times. The School District, therefore, reserves the right to access, inspect, and review any computer, device, telephone system, voice mails, or electronic media within its systems and any data, information, or messages which may be contained therein. All such data, information, and messages are the property of the School District.

Staff members have no privacy interest in the contents stored on or accessed through, or in the internet activity of, the computers, computer network or messaging systems of the District. The District may search files, folders, pictures, video, internet activity, internet cache, web history, or any data stored on or accessed by the computers, computer network, or messaging systems at any time.

Standards of Behavior for All Staff Online Activity

The laws, professional expectations, and guidelines for interacting with students, parents, and other members of the District community that staff members are expected to follow also apply to their online activity. This includes participation in social media sites, such as LinkedIn, Twitter, Facebook, YouTube, and MySpace, or blogs, wikis, and other forms of user-generated media.

Staff members are personally responsible for any inappropriate or illegal content they publish on social media sites. Staff members are prohibited from connecting with current students on social networking sites unless that social network site is provided by the school district, or unless the student is a family member of the staff member.

Staff members must always follow the prohibition against releasing education records or personally identifiable information as set forth in FERPA and other state and federal laws regarding student privacy.

AGREEMENT

I have read the "Staff Network and Internet Acceptable Use and Safety Policy and Agreement" relating to staff use of computers, computer networks, messaging systems, electronic mail (e-mail) systems, Internet, web, or online services in the School District.

I would like to be given access to the School District's computers, computer network, and any messaging systems.

I agree to comply with the "Staff Network and Internet Acceptable Use and Safety Policy and Agreement" and understand that access to the computers, computer network, and messaging systems is a privilege which may be withdrawn in the event of noncompliance with the above Policy.

I also understand that further disciplinary action may result by not following the Policy.

I also understand that the District reserves the right to access, inspect or monitor any of the computers, computer network, Internet, and/or messaging systems of the District.

_____
Staff Member Signature

_____
Printed Name

_____
Date

****

OFFICE USE ONLY

Login Name: _____

Password: _____

Adopted: October 11, 2011