Acceptable Use Policy for Employees

Executive Summary

Computing is an integral part of the academic and business functions of the school district. Many school district functions that an employee encounters in carrying out their job and duties will require that employee to interact with the computing infrastructure and available resources. The computing resources at Dixon Public Schools are the property of Dixon Public Schools. Dixon Public Schools reserves the right to take all necessary measures either proactively or in reaction to an event or the possibility of an event to protect those computing resources.

This document outlines the basic expectations of Dixon Public Schools on how each employee will interact with the district computing systems. Each employee is expected to conduct their computing use in a manner that in no way jeopardizes the availability of the district system or any connected system whether owned by the school district or some other entity. Additionally, Dixon Public Schools strictly prohibits the use of its computing facilities to engage in, participate in, or be party to any illegal activity. The school district will monitor its systems in order to protect against such activity. Additionally, school district employees are exposed to and have access to sensitive data and information, it is expected that the employee will take every known action to protect the privacy and sensitivity of those resources and information.

Any violation of this policy will result in corresponding disciplinary action by the school district. Employees suspected to be in violation of this policy will be reported to the appropriate authorities.

All employees of Dixon Public Schools are expected to be familiar this policy and agree to adhere to it prior to using any computing related facilities. Acceptance will be considered as a condition of employment with the school district.

Purpose

The purpose of this policy is to protect the Information Technology resources and the data that is contained in, or manipulated by those IT resources as used in the daily employment duties of the school district employee. The equipment, software and data used by each employee are expensive and vital assets of Dixon Public Schools that it is the duty of every employee to protect. In addition, Federal and State statutes protect the privacy of much of the information available on school district computer systems.

Policy

It is the policy of Dixon Public Schools that: Dixon Public Schools computing resources are the property of Dixon Public Schools to be used for school district-related business. Employees have no expectation of privacy when utilizing school district computing resources, even if the use is for personal purposes. The school district reserves the right to inspect, without notice, the contents of computer files, regardless of medium, the contents of electronic mailboxes and computer conferencing systems, systems output, such as printouts, and to monitor network communication when:

1. It is considered reasonably necessary to maintain or protect the integrity, security or functionality of school district or other computer resources or to protect the school district from liability:
2. There is reasonable cause to believe that the users have violated this policy or otherwise misused computing resources;
3. An account appears to be engaged in unusual or unusually excessive activity; and
4. It is otherwise required or permitted by law. Additionally, the user name and computing services of the individuals involved may be suspended during any investigation of misuse of computing resources.

General Guidelines

All data pertaining to student records, school district administration, any Federal or State information, and any other information not explicitly deemed public shall be considered confidential and will be safeguarded by each employee having access to that data. All employees will adhere to Federal and State laws concerning privacy. Official releases of data under Freedom of Information requests are to be routed through Central Office.

All school district data, public or private, will be stored in such a manner as to reasonably protect it from loss due to equipment failure, fire, theft, sabotage or human error.

Any computer tape, disk (hard drive, CD or floppy) or other storage medium used to store sensitive school district data must be totally erased or rendered unreadable before it is discarded or disposed of through property transfer or surplus. Employees should contact the Technology Department through the Help Desk for assistance if necessary.

All employees will safeguard their computer user names and passwords. No employee will allow unauthorized persons access to school district data or computing or network resources by sharing their user name and password

No employee will knowingly create access into the computing network in such a way as to bypass the school district security systems. Employees will make reasonable efforts to insure that no software or hardware under their control allows unauthorized access to school district data.

No employee will attempt to use the school district network to gain unauthorized access to other computing resources or data, nor will they knowingly attempt to disrupt the operation of any computer system or network.

No employee will knowingly violate software licenses or copyrights during the course of their job duties or at any time while using district equipment or software. Employees are responsible for producing proof of license for any software installed on their school district-supplied computer. Licenses for personally-owned software installed on a school district computer must be kept with the district technology director.

No employee will use school district data, computing resources or the network for illegal activities or for personal gain.

All employees will safeguard the software and data resources on their workstation or personal computer by installing school district-licensed virus protection software.

All employees will do their best to ensure all software or data is virus-free before it is installed or loaded on a school district computer system. Any detection of a software virus will be reported immediately to the Technology Department through the Help Desk.

No employee will use the school district email system to falsify the identity of the source of the messages; send harassing, obscene or other threatening email; attempt to read, delete, copy, or modify the email of others without their authorization; or send, without official school district authorization, "for-profit" messages, chain letters, or other unsolicited "junk" mail.

Disciplinary Sanctions

The school district will impose disciplinary sanctions on employees who violate the above policies. The severity of the imposed sanctions will be appropriate to the violation and/or any prior discipline issued to that employee.

I understand that should I commit any violation, my access privileges will be revoked, and school disciplinary action and/or appropriate legal action will be taken.

Social Media and Educational Networking

Technology is ever evolving, and as educators, we must utilize tools that will benefit our students' learning. Social networking and educational networking are different tools that should be used appropriately with students. Definitions and examples are provided below. When in doubt, please communicate with administration and seek further guidance on appropriate educational use of these tools.

Social networks are rapidly growing in popularity and are being used by all ages. The most popular social networks are web-based, commercial, and not purposely designed for educational use. They include sites like Facebook, MySpace, Bebo, and Xanga. For individuals, social networking sites provide tremendous opportunities for staying in touch with friends and family as. Educational networking sites are also rapidly growing and are being utilized in classrooms all over the country. These sites are used by educators for both professional development and as a teaching tool. These tools, much like specific parts of Edline, are usually restricted to selected users and are not available to the general public. These include networking tools such as Moodle, educational wikis, Google Apps for Education, specially created Nings, or district adoptions of online applications such as Edline.

As educators, we have a responsibility to use these tools appropriately maintaining our professional image. Our online choices have an impact on our professional image. Other professions are not under the same scrutiny that teachers and other staff members at schools are; because we work with children every day it is essential that we act in a manner that reflects this responsibility. As reported by the media, there have been instances of educators demonstrating professional misconduct while engaging in inappropriate dialogue about their schools and/or students or posting pictures and videos of themselves engaged in inappropriate activity online. Once something is digital online, it is public information that you can not take back. Our online identities are very public, impact our professional image, and can have irreversible results (some of which are undesirable).

One of the biggest decisions of online networks, both social and educational, is the ability to "friend" others – creating a group of others that share interests and personal news. The district strongly discourages teachers from accepting invitations to friend students within personal social networking sites. When students gain access into a teacher's network of friends and acquaintances and are able to view personal photos and communications, the student-teacher dynamic is altered. By "friending" students, teachers provide more information than one should share in an educational setting. It is important to maintain a professional relationship with students to avoid situations that could cause any disruptions to the educational environment.

The district does recognize the value of student/teacher interaction on educational networking sites. Collaboration, resource sharing, and student/teacher and student/student dialogue can all be facilitated by the judicious use of educational networking tools. Such interaction can greatly enhance the learning opportunities in the classroom and spur on additional conversation. As these tools are continually growing and add value to the educational environment, the following guidelines are based on best practices to protect the students, yourself, and the district.

For the protection of your professional reputation, the district recommends the following practices:

Guidelines for the use of social networking sites by professional staff:

- Do not accept students as friends on personal social networking sites. Decline any student-initiated friend requests. Talk with the student the next time you see them about how online friendships are discouraged by the District.
- Do not initiate friend requests with students .
- Remember that people classified as "friends" have the ability to view, download, and share your personal information with others.
- Post only what you want the world to see. Imagine your students, their parents, your administrator, visiting your site. On a social networking site, basically once you post something it may be available, even after it is removed from the site.
- Visit your profile's security and privacy settings. At a minimum, educators should have all privacy settings set to "only friends". "Friends of friends" and "Networks and Friends" open your content to a large group of unknown people. Your privacy and that of your family may be at risk.

Guidelines for the use of educational networking sites by professional staff:

- Let your administrator, fellow teachers and parents know about your educational network.
- When available, use school-supported networking tools.
- Do not say or do anything that you would not say or do as a teacher in the classroom. (Remember that all online communications are stored and can be monitored.)
- Have a clear statement of purpose and outcomes for the use of the networking tool.
- Establish a code of conduct for all network participants.
- Do not post images that include students without parental release forms on file.
- Pay close attention to the site's security settings and allow only approved participants access to the site.

Guidelines for *all* networking sites by professional staff:

- Do not use commentary deemed to be defamatory, obscene, proprietary, or libelous. Exercise caution with regards to exaggeration, colorful language, guesswork, obscenity, copyrighted materials, legal conclusions, and derogatory remarks or characterizations.
- Weigh whether a particular posting puts your effectiveness as a teacher at risk.
- Due to security risks, be cautious when installing the external applications that work with the social networking site. Examples of these sites are calendar programs and games.
- Run updated malware protection to avoid infections of spyware and adware that social networking sites might place on your computer.
- Be careful not to fall for phishing scams that arrive via email or on your wall, providing a link for you to click, leading to a fake login page.
- If a staff member learns of information, on the social networking site, that falls under the mandatory reporting guidelines, they must report it as required by law.

Resources used for the creation of this and sites you can use to further educate yourself:

- A Teachers Guide to Using Facebook, Bernadette Rego http://www.scribd.com/doc/16957158/Teachers-Guide-to-Using-Facebook-Read-Fullscreen

- Connections for Learning: a White Paper. Saywire, 2009 https://saywire.com/downloads/Saywire-White-Paper.pdf
- Educational Networking Articles http://www.educationalnetworking.com/Articles
- Google Apps for Education http://www.google.com/a/help/intl/en/edu/k12.html
- Should Students and Teachers be Online Friends?, Cheri Lucas http://www.education.com/magazine/article/Students_Teachers_Social_Networking/
- Social Networking Best Practices for Educators, http://www.willard.k12.mo.us/co/tech/Document/SocialNetworkBestPractices.pdf

When in doubt please discuss your online activity with a member of the administration. If there is something of question that you encounter on your networking site that could compromise you professionally please let us know about it immediately.