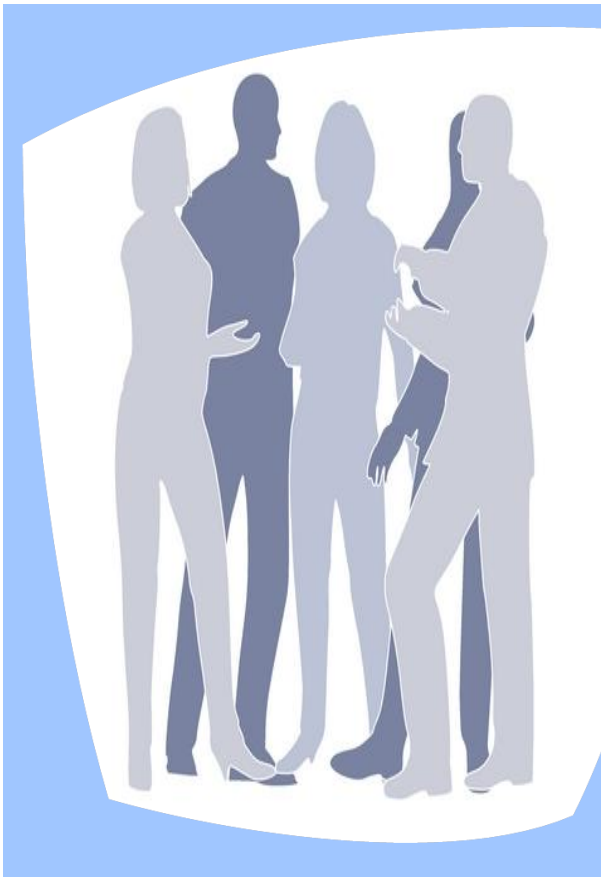
Issue 2 | Vol. 17 | 2010

EduTech In-Focus

EMPOWERING EDUCATORS TO CREATE NEW CONNECTIONS

The risks of implementing open communication services and procedures can invite a variety of dangers including, information security, public relations image issues, communication risks, and others.

Digital Collaboration ~a *Risk Assessment*



By: Ryan Cameron

Although workplace collaboration can bring forth a great deal of positive and needed change within an organization, these changes must be approached with caution. Before the advent of social networking technologies and blazing fast data transfers, most secure documents were kept in a filing cabinet, under lock and key. Now, almost anyone who is comfortable using a computer and sending email can access millions of documents that may or may not be placed under some form of security.

Almost every new technology introduced in recent years has been under scrutiny from top security firms. It seems like every day a new news story is published where information leaks and compromises took place where millions of records are missing or stolen. Technologies such as flash drives, virtual networks, instant messaging, laptops and even high speed file sharing has created an avenue and transport method for sensitive documents and files to be moved quickly and in some cases even anonymously!

Simple Security Tips

1. **Identify** your data and critical information. Take an inventory of sensitive information.

2. **Isolate** and segregate sensitive data. Store information on the fewest number of devices.

3. **Encrypt** sensitive data. Many encryption options are readily available.

Approach Collaborative Technologies with Caution

"If the technology should fail, does that mean the communication will also fail?"

Collaborative technologies can not only result in a security risk, they can also affect workplace communication negatively when they fail. Electronic communications often become a crutch and a dependency on email, texting and chat has emerged for many universities and schools. If the technology should fail, does that mean the communication will also fail?

Without a back-up plan where typically collaborative methods can continue with the absence and or failure of technology, projects may come to a screeching halt!

To maintain an effective information security program, organizations need plans for responding to adverse situations that could affect the confidentiality, integrity, and availability of their information and collaborative information technology systems.

Plans such as contingency and computer security incident response plans must be maintained in a state of readiness to handle potentially harmful events. Instructors and staff members should be trained to carry out their responsibilities, despite a loss of service. Systems and system components should be tested to ensure proper operation when adverse events occur, and plans should be exercised to validate their effectiveness.

Having a sound and practiced security policy in place and employing common sense will add value and ensure the useful effectiveness of any collaborative tool your school utilizes.

OPEN I.T. ENVIRONMENTS: Shared Responsibilities

Establish a culture and plan where everyone has an active role protecting data. It is the responsibility of every computer user to maintain their computer or "lock it down" against viruses, hackers, malicious software, and any other threats which jeopardize the integrity of a network's security.