DETS Web Standards Committee

December 17th, 2010
Agenda
1:00pm – 3:00pm
District 8th Street Annex, Conference Room 1 & CCCConfer

X Ana Bojorquez	_ Marty Licerio	_ Kristi Simonson
X Jason Brady (Chair)	X Alisa Moore	X Yvette Tram
X Rick Hrdlicka	X Craig Petinak	
X Jack Jackson	_ Snezana Petrovic	

TOPIC	DISCUSSION	FURTHER ACTION
Approve Minutes – 9/24/2010	1st –Rick Hrdlicka 2nd –Craig Petinak	
Computer Usage Policy/Administrative Procedure – Review and suggest changes	Changes recommended for Social Media section	
Recommendation for acceptable use of social websites policy	Material provided by Craig Waiting until next meeting to see what Alisa brings from her seminar in January	
Recommendation for appropiate use of external links from district-owned websites policy	Computer and Network Use policy as recommended should cover external links and that the separation of external links is not necessary at this time.	
Proposal for Cross-Referencing on Web Presences	Recommend that information about the relation with the district and all it entails be on the site, recommended be under the about page or the home page. Where studens are looking for information about classes or programs, we recommend that the website recommend the other college if the student can't find what they are looking for.	
Web Compliance & Monitoring Tool Report – Jason Brady	Moving forward for January Board Meeting. Funding provided by EduStream.	
SBVC Website Redesign Report – Jason Brady	Moving forward. HTML templates have been created. Mind Over Media implementing in their Sitecore development instance this month. Updated schedule at next meeting.	
SharePoint – training report, current usage report, future discussion – Jason Brady	After training in November, those who were at the training decided to put the IT directors of each site in charge of handing out permissions (Wayne-CHC, Rick-SBVC, Jeremy-SBCCD). For training, talk with the Profesional development coordinator of your site. I can provide the training book if desired.	
New/Old Business		

Next Meetng – 2/18/2011		

SAN BERNARDINO COMMUNITY COLLEGE DISTRICT
ADMINISTRATIVE PROCEDURES 3720

COMPUTER AND NETWORK USE

Ownership Rights

The San Bernardino Community College District ("District") owns, leases, and/or operates a variety of computer and communication systems, including but not limited to: host computers, file servers, work stations, stand-alone computers, laptops, software, and internal or external communications networks (Internet, email, mass notification systems, telephone and voicemail systems). These systems are provided for the use of District faculty, administrators, staff, and students in support of the programs of the colleges and District. Hereinafter, this system and all of its component parts shall be referred to as the "District Network."

Privacy Interests

The District recognizes the privacy interests of faculty, staff and students and their rights to freedom of speech, collegial consultation, and academic freedom, as well as their rights to engage in protected union and concerted activity. However, both the nature of electronic communication and the public character of District business make electronic communication less private than many users anticipate, and may be subject to public disclosure. In addition, the District Network can be subject to authorized and unauthorized access by both internal and external users. For these reasons, there are virtually no online activities or services that guarantee an absolute right of privacy, and therefore the District Network is not to be relied upon as confidential or private.

District Rights

System administrators may access users' files or suspend services they manage without notice only: 1) to protect the integrity of computer systems; 2) under time-dependent, critical operational circumstances; 3) as required by and consistent with the law; 4) where evidence exists that violations of law or District Policy or Procedures have occurred. For example, system administrators, following organizational guidelines, may access or examine individual files or accounts based on evidence that they have been corrupted or damaged or subject to unauthorized use or misuse. In such cases of access without notice, data or information acquired may be used to initiate or extend an investigation related to the initial cause or as required by law or Board policy and/or to protect system integrity.

System Abuse

Users are prohibited from the use of the access codes of other users to gain access to computer resources on the District network. Users are responsible to safeguard accounts given them. Therefore they should not provide their access codes to others for the purpose of accessing District computing resources.

Users shall not attempt to modify any part of the network, attempt to crash or "hack" District systems, or tamper with any software protections or restrictions placed on computer applications or files. Unless properly authorized, users shall not attempt to access restricted portions of any operating system,

security software, or application system. District computing resources may not be used to violate copyright laws or license agreements.

Harassment

Users are prohibited from using the District's information systems in any way that may be disruptive or offensive to others, including, but not limited to, the intentional viewing and/or transmission of sexually explicit messages, graphics, cartoons, ethnic or racial slurs, or anything that may be construed as harassment or disparagement of others. This is consistent with the District's non-discrimination policy.

Commercial Use

Commercial use of the District computing resources for personal gain or illegal purposes is prohibited. Computer resources on the District network are provided to support District-related academic and administrative activity. They may not be used for the transmission or storage of commercial, political, or personal advertisements, solicitations and promotions, destructive programs (viruses and/or self-replicating code), or any other unauthorized use. Transmitting unsolicited advertising, promotional materials or other forms of solicitation are prohibited without prior authorization by District administration.

Fair Use

Information appearing on the internet should be regarded as copyright protected, whether or not it is expressly noted as such. Section 107 of the Copyright law (title 17, US Code) allows for Fair Use of copyrighted materials. Teaching, scholarship, research, comment, news reporting, and criticism are considered fair and allow for reproduction of a given work. Acknowledgement of the source is recommended but is no substitute for obtaining permission (http://www.copyright.gov/fls/fl102.html).

Software Licensing

Software, used on District owned computers, must be properly licensed. These licenses provide the acceptable use of the software and hold the user and in some cases the District legally responsible for copyright violations.

All software must be approved by district and/or campus technology departments prior to purchase. Software, its associated license material, and proof of purchase will be submitted and stored with district and/or campus technology departments. For specific District purchasing procedures, please refer to Administrative Procedure 6330.

Exceptions

Activities will not be considered misuse when authorized by appropriate District officials for security or performance testing. Technology support staff, under the direction of senior management, may at any time examine the equipment, software and services of District owned equipment.

Technology support staff monitors for any unauthorized equipment or software on the District's networks, and reserve the right to remove, disconnect, or disable the unauthorized equipment or software.

Network Access, Media and Social Networking

SBCCD provides network and telecommunications services as a tool for students, staff and faculty. Internet access is provided to assist in the completion of college related work and assignments. As such, the district provides this service and is subject to state and federal regulations. This applies to all equipment attached to the provided network, wired or wireless, without regard to ownership of the equipment.

Personal social networking accounts shall not be used to officially represent campus or district entities on social networking, wiki, or other social media sites. For official representation of any District entity, a~~n approved~~ campus or district account, approved by the president/chancellor or their designee, must be used. The account holders must agree to use the resources legally, ethically and in keeping with the intended use per the procedures of their respective sites.~~.~~

PDA and Smartphones

SBCCD does not provide support for PDAs and smartphones. SBCCD only provides the connection settings to the Exchange messaging system for the synching of SBCCD e-mail, calendar and contacts on smartphones and PDAs. It is the user's responsibility to enter the settings or get the services provider to enter the settings.