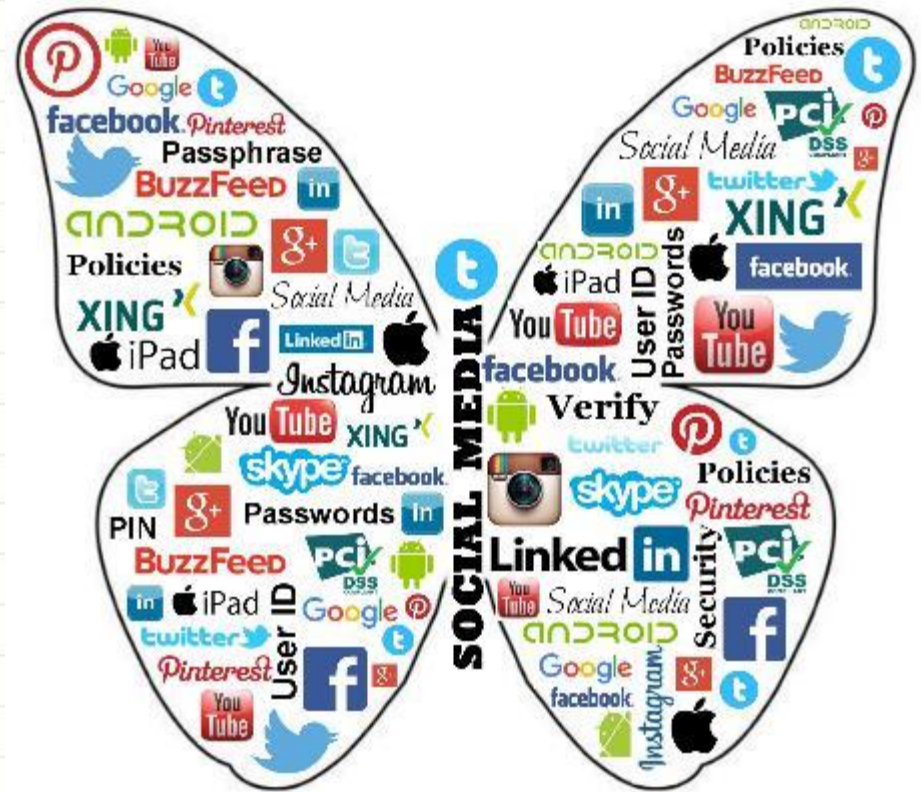


TECHNOLOGY SERVICES FOR FACULTY



Deborah Ludford
October 6, 2017
New Faculty Orientation

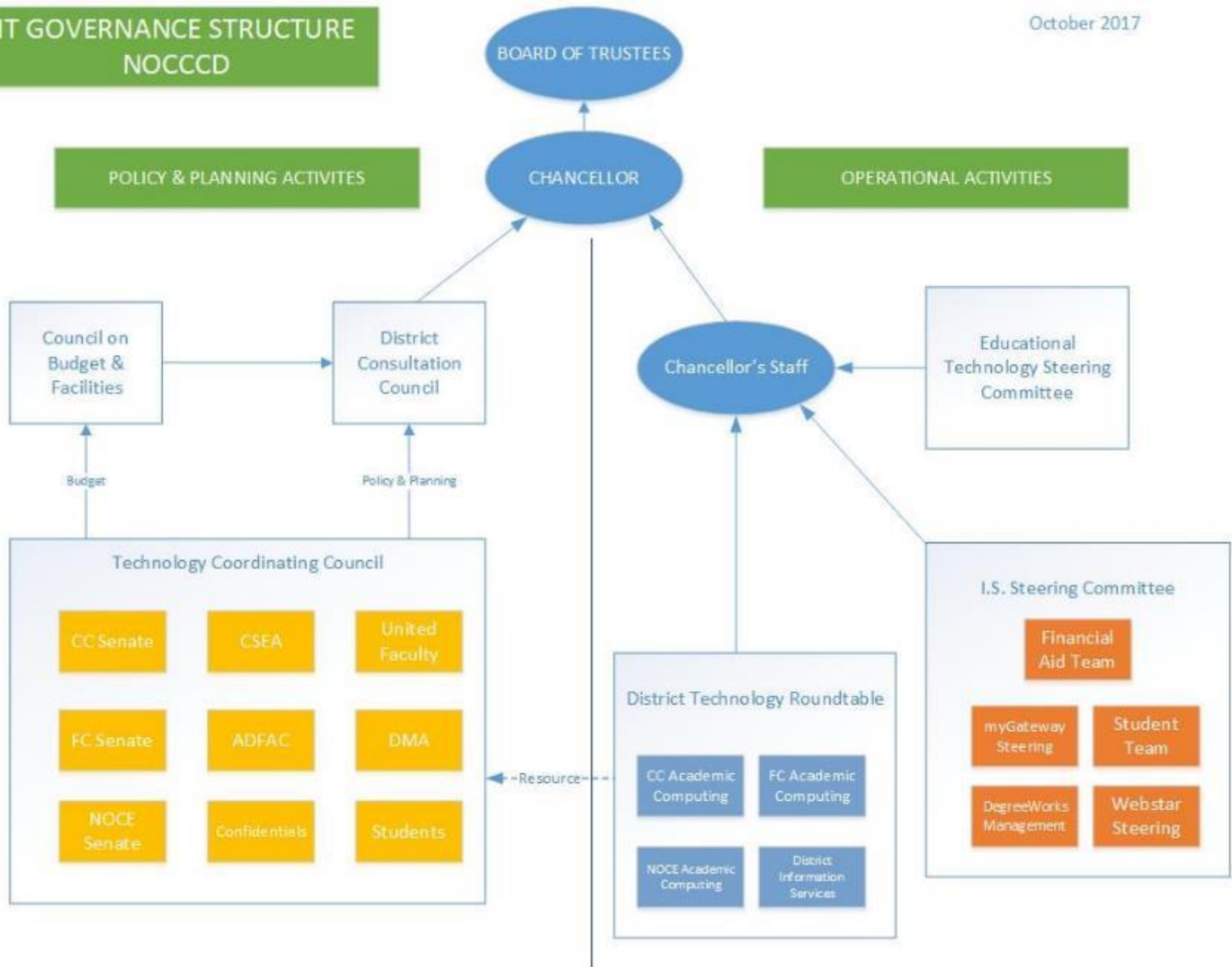
Agenda



- Technology Services provided by the District and Campus
 - IT Governance
 - Technology Services
- Classroom tools
 - Cloud Services
 - Social Media
 - E-mail
 - Websites
 - Mobile Devices
 - Print Materials/Copyright and reposting of digital items
- Resources
- Questions?

IT GOVERNANCE STRUCTURE NOCCD

October 2017



Technology Services



- Campus – Academic Computing Technologies
 - Classroom support
 - Desktop/laptop support
 - Consultation on software and hardware
 - A/V support
 - Email support
 - Access systems support
 - Web pages for faculty and departments
- [Fullerton College Faculty/Staff](#)
- [Cypress College](#)
- [NOCE](#)
- District – Information Services Department
 - Administrative systems including student, finance, HR, financial aid and 54 others
 - Systems used by all:
 - Qualtrics-surveys
 - Lynda.com-training
 - MSDN-Microsoft
 - Gartner-research
 - Grades
 - Employee systems for benefits, pay information
 - myGateway Portal
- [NOCCCD](#)

Why do we care about Safety?



- According to Osterman Research, Inc. the **typical** information worker **spends 153 minutes per day working in email and 51 minutes in social media – 42.5 percent of a typical eight - hour day**
- During just the last 12 months:
 - **74** percent of organizations have been infiltrated with malware through **Websurfing**
 - **64** percent have experienced malware infiltration through **email**.
 - **22** percent have experienced an accidental or malicious leak of sensitive or **confidential data through email**
 - **14** percent of organizations have had malware enter the corporate network through **social media or other Web 2.0 apps**
- Reference: [Best Practices in Email, Web, and Social Media \(Trustwave\)](#)

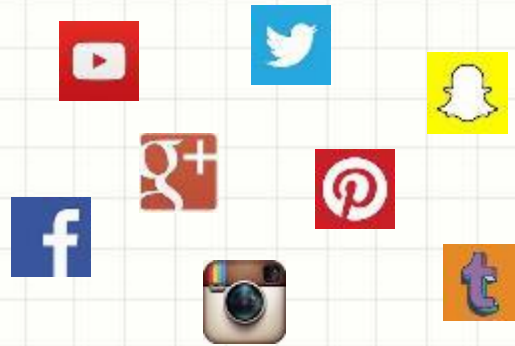


Cloud Services



- Most new development of systems is offered in the cloud as the only option – Why?
- Once something is in the cloud even if you delete, it is not gone!
- Only protection is the contract / End User Licensing Agreement – Read it!
- Reference: [Cloud Solution Security Measure Guidelines](#)





Social Media



- [Top 7 Social Media Security Practices](#)
- Separate Work from Personal – e-Discovery; Free Speech; Privacy
- Understand how security settings work
- Restrict your posts to the intended audience
- Just because you delete something, it isn't truly gone – everything is stored on a backup server somewhere
- Social Media is a cloud based service in most cases, treat it as such
- If you don't want it seen on the front page of the paper or in a Tweet, don't write it!
- Reference: [Social Media Guidelines](#)
- Video: [Internet Privacy](#)



Email



- What is [phishing](#)? Does someone possess enough personal information to pose as you?
- Do not open ANY attachments that you cannot recognize or end in .exe or .scr
- Do you know the person? Are you expecting them to send an attachment? Call and ask.
- Never send passwords, credit card, SSN etc.
- Don't send anything you don't want to see in the newspaper or on Twitter!



Websites



- Anything on a public site is available to the world!
- Remember, you are representing the District if you use a website for District business
- Reference: [Website Guidelines](#)
- Don't forget ADA/Section 508 requirements! Contact campus DSS office for assistance.



Mobile Devices



- District Owned Devices governed by BP/AP 3720
- Personal devices or BYOD (Bring Your Own Device)
 - Use is optional
 - No official technical support
 - Wired or wireless network use is governed by each campus
 - Do not expect privacy
 - BP 5500 will apply to your students' usage
 - Include expectations for mobile devices in your course syllabus; you cannot require them of students
 - Wipe your mobile device of college business upon separation
 - Do not share personal information
 - Contract provisions will apply
- Use of personal device may become public if used for business!
- Reference: [Mobile Computing Device Guidelines](#)



Print Materials



- District copyright governed by BP/AP 3750
- Link when possible – check online or library
- Fair Use – understand if it is covered
- Reference: [Know Your Copyrights](#)
- A few words on using images...



Federal and State Laws



- **FERPA** -The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.
- **HIPAA** - Privacy Rule which creates national standards to protect individuals' medical records and other personal health information.
- **California Breach Notification** - Protects Personally Identifiable Information.
 - State Agencies
 - Businesses
- **Privacy, etc.....it is also just the right thing to do!**

Local Policies & Guidelines



- Be familiar with the district and know what is expected
- Board Policies and Procedures
 - [Computer Use](#)
 - [Websites](#)
 - [Copyright](#)



A Few Other Reminders!



- [Ransomware](#) - The newest threat.
- Do not share passwords! Violates Board Policy.
- Do not use personal information when creating a password. Consider using a phrase instead.
- Computers – log off/turn off when leaving work.
- Resource: [Creating A Strong Password](#)
- Video: [What is your Password?](#)



Additional Resources



- ❖ [California Community College Legal Opinions](#)
- ❖ [Chancellor's Office Legal Advisories](#)
- ❖ [ADA/Section 508 – Chancellor's Office](#)

For Assistance



Contact information:

I.S. Helpdesk

ishelpdesk@nocccd.edu

(714)808-4849

Questions?

Thank You!