Roundtable

FOOTHILL COLLEGE

OCTOBER 15, 2008

Purpose: **Participatory Governance Leaders Meeting**
Location: **President's Conference Room**
Time: **1st & 3rd Wednesday - 1:30 p.m. to 3:00 p.m.**

Roundtable 1A (2008-09) – Ed Master Plan
  Leadership Development/Learning Outcomes for Roundtable Members
  Presentation Skills Development
  Knowledge of FH Ed Master Plan
  Advanced Knowledge of RT Missions
  Ratification of Basic Skills Action Plan
  Ratification of Sustainability Plan
Roundtable 1B (2009-10) – "B" is for Budget
Roundtable 1C (2010-11) – Accreditation Self Study

DATE	AGENDA TOPIC	DISCUSSION LEADER	EXPECTED OUTCOME
Oct. 1	Welcome Reception Leadership Orientation/Community Building/Mentorships 1st Reading of RT Guidelines Revisions	 Miner Miner	Enjoy! Annual Orientation Introduce revisions
Oct. 15	Ed Master Planning Introduction Program Planning 2nd Reading of RT Guidelines 2nd Reading of Mission/Vision Statement Security Policy	Miner/Lamanque Graham Miner Miner Miner	Understanding of planning process Understanding of planning process Endorse changes Submit revisions Review for feedback
Nov. 5	Basic Skills		Intro of action plan
Nov. 19	Basic Skills LeaderFISH – "It Begins With Me"	 Stenger	Endorse plan Leadership Development
Dec. 3	Wrap up and Evaluation of Fall Quarter "Work" Report from Sustainability Committee Adjourn to Holiday Party	Miner Visas	Evaluation Activity Update Celebrate!
Jan. 7, 2009	Student Recruitment & Outreach	Harrall, Hamp Haywood-Smith, Galope	Intro of action plan
Jan. 21	Student Recruitment & Outreach	Harrall, Hamp Haywood-Smith,	Endorsement of plan

	LeaderFISH – "Be There"	Galope Stenger	Leadership Development

Feb. 4	Voc Ed	Violett, Murphy FA Dean,Galope, Woods, Orrell	Intro of action plan
Feb. 18	Voc Ed	Violett, Murphy, FA Dean,Galope, Woods, Orrell	Endorsement of plan
	LeaderFISH – "Coaching"	Stenger	Leadership Development
March 4	Wrap up and Evaluation of Winter Quarter "Work"	Miner	Evaluation
April 8 Moved from Apr. 1	Student Development & Retention	Cormia, Smith, Dorsey	Intro of action plan
April 15	Directions to RT re: Program Plans	VP Inst. Research	Intro of action plan
	Student Development & Retention	Cormia, Smith, Dorsey	Endorsement of plan
	Transfer	Meezan, Harris, Dorsey, Cellilo	Intro of action plan
May 6	Transfer	Meezan, Harris, Dorsey, Cellilo	Endorsement of plan
	Ed Resources Presentation	Barker	Recommendations for faculty pos.
May 20	Ed Master Plan Review Presidential Report LeaderFISH – "Make Their Day"	Miner Miner Stenger	Revisions? Ratification of faculty positions Leadership Development
June 3	Final Version of Ed Master Plan LeaderFISH – "PLAY"	Miner Stenger	Endorsement of plan Leadership Development
June 1 6:00-7:30	State of the College		Recognition of RT Accomplishments
June 11	End of the Year Celebration – "Leadership Awards"		Let's Celebrate!

IMPORTANT DATES:

April 9 – Program Plans and funding requests due
May 20 – Notification by President of approved faculty positions
June 1 – Foothill State of the College
June 11 – End of the Year Celebration

MISSION
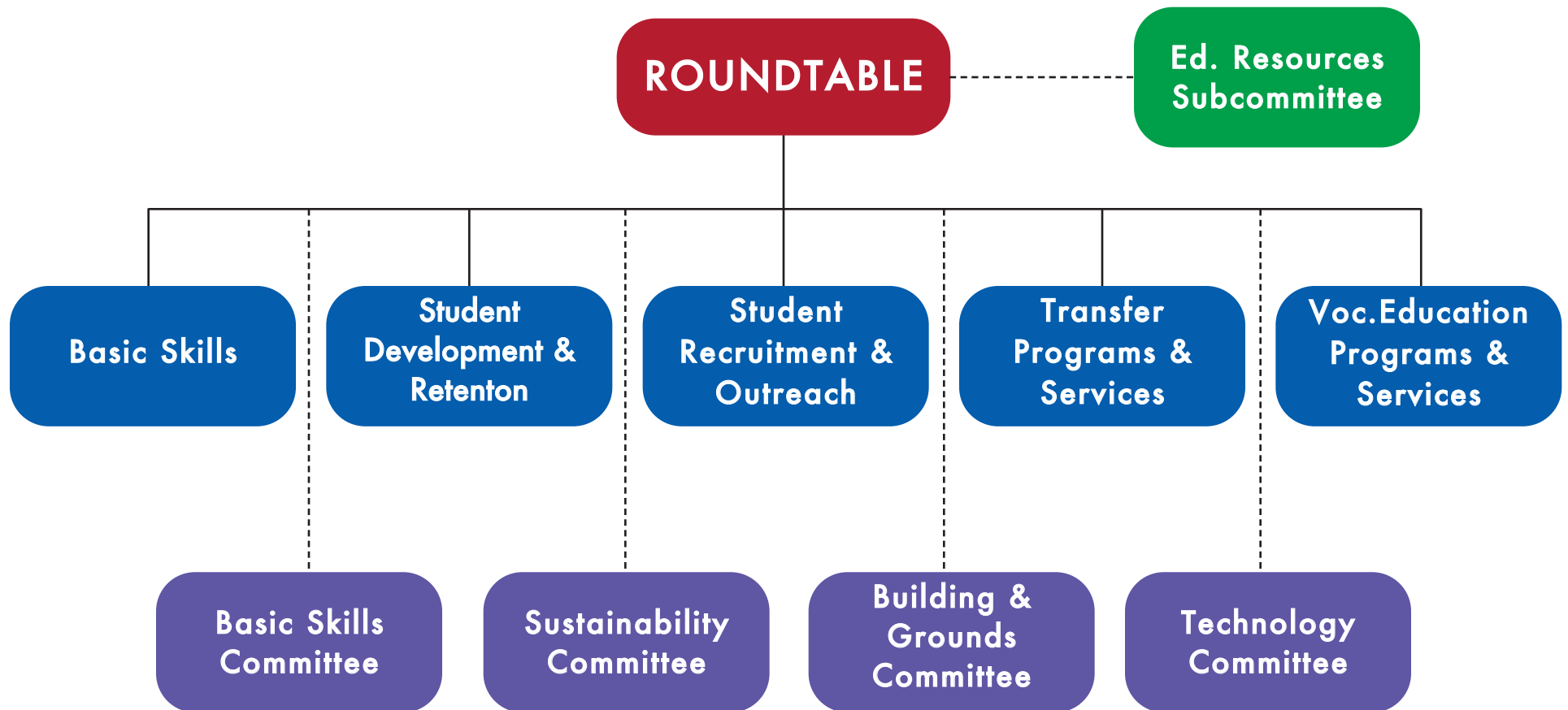
Our mission is to promote student learning through ~~lower division~~ **college level** ~~academic instruction~~ transfer preparation, career preparation, **lifelong inquiry**, and continuous workforce improvement to advance California's economic growth and global competitiveness.

VISION

Students who attend our college achieve their goals because relevant instruction occurs in an engaging, stimulating, inclusive manner, and appropriate support services are provided. Students feel accepted as part of the Foothill family ~~and realize they made the right choice in choosing Foothill to further their~~ **which actively engages in the furtherance of students'** education and personal development.

Revision 10/10/08

ROUNDTABLE ----- **Ed. Resources Subcommittee**

Basic Skills

Student Development & Retenton

Student Recruitment & Outreach

Transfer Programs & Services

Voc. Education Programs & Services

Basic Skills Committee

Sustainability Committee

Building & Grounds Committee

Technology Committee

Last updated 10/09/08

Electronic Information Security Policy
(draft)

Foothill De-Anza Community College District ("District") retains selective personal information in electronic form on employees, students, contractors and other individuals who conduct business with the district. Certain types of personal information, if divulged publicly or to unauthorized individuals, could result in significant personal damage including financial loss, loss of credit standing, or other problems requiring extensive time and effort by the affected individual(s) to address. To protect personal information, state and Federal laws restrict how certain types of personal information can be stored, displayed, or transmitted through electronic networks and in information technology systems. Furthermore, some laws require disclosure when information is compromised or when information systems have been breached.

The District and its employees have an ethical and legal obligation to take necessary steps to protect all personal information that is provided to the District.

The Board directs the Chancellor or designee to develop and implement procedures that will:

1. enforce all existing federal and state laws, including those laws and regulations that are specific to electronic information security as well as apply to the protection of personal information.

2. employ best practices to safeguard the storage and transit of personal information across the District's information systems and digital networks.

3. delineate processes for expeditiously investigating suspected breaches, thefts of computing systems, or inadvertent disclosures of personal information contained in District information technology systems. These processes shall also describe the appropriate follow-on actions to take to limit damage, secure compromised systems, and notify affected persons.

Electronic Information Security Procedure
(draft)

If you suspect that a security breach has occurred in a district-owned computing system, contact the:	
Call Center at x8324 **during work hours**	**District police at x7313** **after work hours / on holidays**

Purpose

The purpose of this procedure is to enhance the security of stored, transmitted, and distributed personal information that could be used to impersonate an individual and cause serious loss of privacy and/or financial damage.

In addition to this procedure, colleges and departments are urged to establish best practices that reduce the collection, distribution, and retention of personal data, which is not necessary to perform the educational and business needs of the institution.

Legal requirements and local policy require that District personnel take appropriate measures to protect personal information from inadvertent or illegal exposure to unauthorized individuals. Other legal requirements require that if certain personal information is inadvertently disclosed, the district / college must notify all individuals whose information was compromised. Refer to the table below for further details regarding legal and local requirements.

Legal and Local Requirements for Safeguarding Personal Information

Reference*	Applies to	Required by applicable law	Requires protection?	Requires notification?
A - 1.	All individuals	California Civil Code 1798.85, 1798.29	Yes	**
A - 2.	Students	Family Educational Rights and Privacy Act (FERPA)	Yes	No
A - 3.	Employees	District procedure	Yes	No

*refer to *Personal Information* definitions below

**Civil Code 1798.29 requires "state agencies, businesses and persons conducting business in California" to notify affected persons in event of a breach. This section of code may not apply to California Community Colleges.

Definitions

A. PERSONAL INFORMATION:

Personal information includes:

1. For all individuals, an individual's first and last name in combination with any of the following:

- social security number
- driver's license number
- financial account or credit card number in combination with any password that would permit access to the individual's financial account
- medical information

2. For students, all personally identifiable information not included as *directory information*. This would include the students name in conjunction with:
   - the <u>name</u> of the student's parent(s) or other family members
   - the <u>address</u> of the student's family
   - a <u>personal identifier</u>, such as a social security number or student number
   - the <u>race</u> or <u>ethnicity</u> of the student
   - the <u>gender</u> of the student
   - a list of <u>personal characteristics</u> of the student
   - academic <u>evaluations</u> and <u>grades</u> of the student
   - transcripts and other <u>academic records</u> of the student
   - <u>scores</u> on tests required for new students
   - the student's <u>class schedule</u>
3. For employees, an individual's first and last name in combination with the:
   - employee's ID number

B. DIRECTORY INFORMATION (FERPA DEFINITION):

Information that is generally not considered harmful or an invasion of privacy if released. The primary purpose of directory information is to allow the District / College to include this type of information from a student's education records in certain school publications. Examples include:
- A playbill, showing the student's role in a drama production
- The annual yearbook
- Honor roll or other recognition lists
- Graduation programs
- Sports activity sheets, such as for wrestling, showing weight and height of team members

C. SECURITY BREACH:

An incident when an individual's <u>unencrypted</u> *personal information* has been (or is reasonably believed to have been) <u>exposed to</u> or <u>acquired by</u> an unauthorized person. (Good faith acquisition of *personal information* by an employee or agent for district / college purposes does not constitute a *security breach*, provided that the *personal information* is not further disclosed to unauthorized persons.) The theft of a *computing system* that contains or may contain *personal information* will be considered a potential *security breach*. Inadvertent access to *personal information* that occurs in the course of performing technical services on a *computing system* by an authorized technical staff member will not be considered a *security breach*.

D. COMPUTING SYSTEM:

Any server, desktop or laptop computer, or PDA that contains (or provides network access to) data files

E. COMPUTER-BASED INFORMATION SYSTEM:

Any computing system that is used in the acquisition, storage, manipulation, management, movement, control, display, transmission, or reception of data (including software, firmware, and hardware), which is used to provide services to persons other than the owner.

F. COMPUTER-BASED INFORMATION SYSTEM MANAGER (CBIS MANAGER):

An individual who maintains and manages an information system, server, or other technology device that stores or transmits data.

G. DATA RESOURCE

Data (information) that is stored on a *computer-based information system*

H. DATA RESOURCE MANAGER:

An individual who controls the use of and access to a *data resource*

I. LEAD AUTHORITY:

An administrator who has been delegated responsibility for oversight of data security at a college or Central Services. Each president will designate a person to act as the *lead authority* for their college. The Vice Chancellor of Technology is the *lead authority* for Central Services.

J. CONTROL RECORDS:

The records contained in a database, spreadsheet, or other electronic file that document system and application level access methods into those computer-based information systems containing *personal information*. Control records must contain the following for each computer-based information system:

- name of the *computer-based information system*
- physical location of *computer-based information system*
- name of the *CBIS manager*
- name of the *data resource manager(s)* who have responsibility for any data containing *personal information* on the *computer-based information system*
- description of logical access methods and security controls (user IDs, passwords, encryption keys, etc.) necessary to gain access to the *computer-based information systems* and its data or, the name of another employee (in addition to the CBIS manager) who has knowledge of logical access methods and security controls (e.g. who can gain access to the system and applications as a systems administrator)

K. ETS INCIDENT RESPONSE TEAM

A team of designated ETS members who investigate and respond to security incidents

Responsibilities

A. THE LEAD AUTHORITY HAS OVERSIGHT RESPONSIBILITIES TO:

- identify *computer-based information systems* under their jurisdiction that contain *personal information* or that provide to access to *personal information*
- ensure that *data resource managers* and *CBIS managers* perform their functions as specified in this document
- create a secure central repository to contain *control records* on *computer-based information systems* that contain *personal information*
- know where to rapidly locate contact information (email and postal addresses) for individuals of whom *personal information* is retained or transmitted. (Contact information on all students and employees is kept in the district's administrative information system.)

- ensure that the incident response process delineated in these procedures is followed (if a security breach occurs on a *computer-based information system* or a *data resource* managed by an individual in his / her organization [college or Central Services]).
- rapidly notify affected individuals whose personal information may have been compromised as the result of a *security breach* of a *computing system* or actions of an employee under the jurisdiction of the *lead authority* as required by this procedure. Current law (as of April 2008) requires that notification be made in *the most expedient time possible and without unreasonable delay*. (Refer to CALIFORNIA CIVIL CODE 1798.29).

B. THE <u>CBIS MANAGER</u> HAS RESPONSIBILITIES TO:

- develop security measures, including District published best practices to reduce vulnerabilities of *personal information* contained in computer-based information systems within their jurisdiction including the use of appropriate encryption strategies for both transmission and storage of *personal information*
- create, retain and secure *control records* for computer-based information systems that contain *personal information*
- annually update *control records* as necessary including those kept in the central repository
- implement procedures and tools to monitor access to computer-based information systems that contain *personal information* and to indicate if unauthorized access occurs
- remove files containing *personal information* (using an industry standard secure data removal tool) from servers, which are identified to be salvaged or repurposed

C. THE <u>DATA RESOURCE MANAGER</u> HAS RESPONSIBILITIES TO:

- grant access to a data resource or data to individuals / positions on a "need to know" basis
- inform individuals who have access to the data resource (and any downstream users of distributed data) of their responsibilities to secure and protect *personal information* as well as to destroy it when no longer needed. Include applicable:
  - o district and college policies and procedures
  - o best practices

D. <u>ALL EMPLOYEES</u> HAVE RESPONSIBILITIES TO:

- abide by the established procedures with regard to accessing and using *personal information*
- protect and secure *personal information* under their control using best practices as outlined in the publication: *Information Security Best Practices* which is available on the FHDA Website
- destroy data containing *personal information* when no longer needed
- See also: *Computer and Network Use: Rights and Responsibilities Policy / Procedures 3250 / AP 3250*

E. OTHER RESPONSIBILITIES

- FHDA District Police will act as the point of contact between the district and external law enforcement agencies when external law enforcement agencies are involved
- ETS shall remove *personal information* (using an industry standard secure data removal tool) from desktop / laptop computers, which are designated to be salvaged or repurposed
  - o System hard drives may be destroyed as an alternate method of removing sensitive information

Incident Response Process

The incident response process consists of the following steps that must be implemented in the event that a *security breach* occurs:

A. NOTIFY KEY PERSONS

If a person suspects that a *security breach* has occurred on a *computing system* that contains or has network access to unencrypted *personal information*, the person identifying the incident must immediately contact the ETS Call Center (during work hours) or the district police (after work hours). If the security breach is reported after work hours have ended, then district police will notify the Vice Chancellor of Technology. The Vice Chancellor of Technology or designee will notify the appropriate Lead Authority.

B. ISOLATE THE SYSTEM

For *Computer Based Information Systems*:

The *CBIS manager* will disconnect the *computing system* from the campus network without modifying any settings, files, etc. on the *computing system,* and leave the system powered up*.*

For employee assigned desktop or laptop computers:

If the computer is turned on, the employee should immediately disconnect the computer from the network (by removing the network cable or disconnecting from a wireless connection). The computer should not be turned on or off or otherwise modified in any way.

For Stolen *Computing Systems*:

If a stolen *computing system* is recovered, the person gaining possession of the system will notify the Call Center, who will arrange for the system to be picked up. The *computing system* should not be turned on or otherwise modified in any way.

C. ANALYZE THE BREACH

The ETS Incident Response Team, in cooperation with District Police (if involved) and the CBIS manager, will look for evidence of a *security breach* to assess the possibility that *personal information* has been compromised

D. REPORT THE INCIDENT

If the ETS Incident Response Team, in cooperation with District Police (if involved) and the CBIS manager, has sufficient reason to believe that *personal information* may have been acquired by or exposed to unauthorized individuals, the ETS Incident Response Team will submit written notification describing the nature of the *security breach* and estimated number of affected individuals to the:

- Chancellor
- President of the college (if applicable)
- Vice Chancellor of Technology
- Lead authority
- District and college (as applicable) communication coordinators
- District Police

E. RESTORE AND RECONNECT THE SYSTEM

The *CBIS manager* may repair and restore system functionality to the *computing system* when:

- The computing system is no longer needed for forensic analysis or police investigation and
- It has been cleaned of all known malware

The *ETS Incident Response Team* will work with the *CBIS manager* and District Police (if involved) to determine when the *computing system* can be reconnected to the campus network

- Special consideration for rapid restoration and reconnection will be given to *computing systems* that provide time sensitive functionality to support critical campus services

F. NOTIFY INDIVIDUALS WHOSE PERSONAL INFORMATION HAS BEEN COMPROMISED

1. Decide if notification is required and how notification will be made

The district / college communication coordinators (as appropriate), the Vice Chancellor of Technology, the *lead authority* and the district's attorney will confer to determine whether or not the criteria for notification under California Civil Code 1798.29 and 1798.82 has been met and to determine which means of notification to use (e. g., email, postal mail, or website notice)

2. *Personal information* not involved

If information beyond the data elements defined herein as *personal information* is accessed by an unauthorized person, the appropriate district / college communications coordinator in coordination with the District's attorney will determine what notification will be made to affected individuals.

3. Required information

If notification is required, the appropriate district / college communication coordinator shall notify affected individuals of the *security breach* and include the following information:

- The date(s) on which the personal information was (or could have been) acquired.
- A description of the personal information, which was (or could have been) acquired.
- The name of the department or unit responsible for the information and the relationship that the affected individual has (had) to the department (in such a way that the person receiving the notification will understand why that department or unit had their information).
- An indication of the likelihood that the personal information was acquired or used.
- An email address and phone number of a suitable college or Central Services representative with sufficient knowledge of the incident to be able to handle questions from affected individuals.
- A list of resources that affected individuals can use to check for potential misuse of their information.
    - This list should include the following flyer (either as a link or a hardcopy attachment): "What to Do If Your Personal Information is Compromised" (http://www.privacy.ca.gov/financial/sbfs021205.pdf), produced by the California Office of Privacy Protection

The appropriate district / college communications coordinator will also determine what additional advice or assistance will be given to the affected individuals.

4. Timeliness of notification

Notification must occur without unreasonable delay, except when a law enforcement agency has determined that notification will impede a criminal investigation. (In this case, notification must occur as soon as the law enforcement agency determines that it will not compromise the investigation)

5. Substitute method of notification

If sufficient contact information is not available for direct hard copy or e-mail notice for some affected individuals, a substitute method of notice may be used. The substitute notice should include a prominent display on the campus' Web site or other commonly used Web site for at least forty-five days.

6. *Submit the After Notification Report*

The district / college communication coordinator will provide a written report describing the number of individuals successfully notified, the number of individuals for unsuccessful notifications, and which methods were used for notification, along with any issues that have arisen as a result of the breach such as press coverage, complaints from affected individuals, etc. The report will be sent to the following individuals:

- Chancellor
- President of the college (if applicable)
- Vice Chancellor of Technology
- Lead authority
- District communication coordinators

References

- Information on privacy laws applicable to California
  http://www.privacy.ca.gov/lawenforcement/laws.htm#twelve
- Important legislation governing the security of confidential information
  - o Health Insurance Portability and Accountability Act of 1996 (HIPAA) - 45 CFR Parts 160 and 164
  - o Family Educational Rights and Privacy Act of 1974 (FERPA) - 20 U.S. Code section 1232g
  - o Breach Notification Law: California Civil Code - 1798.29 (previously SB1386)
  - o Security of Personal Information: California Civil Code - 1798.85 (previously SB 25)
- FHDA - AP 3410 Guidelines for Classification, Retention and Destruction of Records
  http://fhdafiles.fhda.edu/downloads/aboutfhda/3410ap.pdf
- FHDA - Policy 3250 / AP 3250 Computer and Network Use: Rights and Responsibilities
  http://153.18.96.19/downloads/etac/Policy3250.doc%20
- FHDA – Policy 5050 Furnishing Information Concerning Students
- FHDA – Policy 4150 Personnel Files
- Information Security Best Practices www.fhda.edu/security