Library, Media, and Information Services Committee
Meeting Notes for 10/20/2017

Present: Sam Berling, Jane Carlin, Kate Cohn, Sue Hannaford (Chair), D. Wade Hands, David Latimer, Janet Marcavage, Ann Gleason, and Lisa Wood (Note-taker)

The meeting was called to order at 1:04 p.m.

The minutes from 10/6/2017 were approved with minor corrections.

New Business:

1. Discussion of the Campus Directory was deferred until next meeting in order to include Jeremy Cucco.

2. The committee resumed its discussion of security practices around storage, retention, and purging of institutional data by faculty and staff. Prior to our meeting, Jane Carlin circulated several security practice documents that she collected from varied academic institutional websites.

Latimer noted that the UC Santa Barbara document seemed most closely aligned with goals identified in our previous discussion, particularly the information on specific security practices for faculty and staff. Several faculty agreed that a brief set of guidelines would foster a visible campus culture concerning document management and security. Over the course of our discussion, the committee identified a number of specific information management practices including:

- Providing guidelines for sorting, storing, and purging sensitive documents.
- Setting an annual document clean-up day, where campus members delete or shred confidential documents that are no longer needed.
- Determining detention time lines (possibly 3-5 years) for retaining on-line course materials that have student information, such as grading records on Moodle.

There was general agreement about the value of a brief document outlining best practices in data security for faculty and staff, including legal requirements about security of student data.

Prof. Hands mentioned that many faculty would be in favor of changing how they manage student information, but might not know what strategies to use. He added that raising awareness of these issues would likely lead to greater conscientiousness.

The conversation turned to broader concerns about data security, and protections in the event that individuals or other entities (legal or private) request information about

students, faculty, or staff. The general consensus was that privacy of campus members should be protected when permission has not been given to release information.

Kate Cohn defined a clear distinction between legal requirements (FERPA Family Education Rights and Privacy Act) for protecting the confidentiality of student information, and ethical practices that might vary depending on the situation and preferences of individual faculty and staff members. She added that requests about student citizenship status should be handled by following guidelines released earlier this year. Any requests for information made by Immigration and Customs Enforcement (ICE) should be referred to one of the contact people listed below if the issue arises during business hours, and to Security Services between 5 p.m. and 8 a.m.

People to Contact if ICE requests information:
Dave Wright, University Chaplain ext. 2751
Cindy Matern, Associate VP for Human Resources ext. 3116
Michael Pastore, University Registrar ext. 3529
Todd Badham, Director of Security Services ext. 3311
Security Services: ext. 3311

Anne Gleason addressed a number of questions concerning policies and practices around protection of student and faculty information, including limits of access by information services. First, she stated that the information services cannot log onto university issued/owned computers without permission from the faculty or staff member that uses that computer. She added that extra encryption has been added to university desktops and laptops so that data is more secure, and that our firewall is designed to protect our data from outside breaches. With regard to data collected by the university on campus use of the internet, she explained that any information left on the server regarding campus members' usage is removed quickly due to space considerations.

The question of private data stored on campus computers (e.g. bank account numbers, payment details) was raised in regard to confidentiality. Carlin and Gleason stressed that personal information related to non-academic business is best kept on non-university computers, noting that email can be subpoenaed. Hands suggested that the line between personal and professional is not easily drawn when professional and personal roles overlap, e.g. when close colleagues are also friends. Several committee members added that this would be a useful topic to address in a document defining best practices.

The meeting adjourned at 2:00 p.m.

Respectfully Submitted,

Lisa Fortlouis Wood