Pomona College has both legal and ethical obligations to protect the information that it gathers and maintains about its students, staff, and faculty, and compelling operational reasons to maintain control over “instances” of such data in our information systems. Unauthorized access to information – most particularly personally identifiable information (PII) could subject the College to undesirable liability, costs, and damage to our reputation, and uncontrolled duplication of data could lead to embarrassing and awkward errors. Nevertheless, new electronic applications that operate “in the cloud” are being developed to accomplish specific business functions, and some of these require uploading information from college databases to outside entities. Implementing such applications requires careful analysis and safeguards in order to protect the PII for which we are responsible.

The procedures to be followed to authorize release of personally identifiable information (PII) from the college’s information systems to outside entities are described below. Current instances of such release involve either required governmental processes (e.g., SEVIS data collection), established research entities (e.g., COFHE), or business functions that require outside functionality (e.g., benefits administration) but, increasingly, we will be facing questions about more routine functionality. (For example, one option being considered for the future is outsourcing of the Sakai function.)

The premise of what follows is that transfer of PII collected and maintained on college-operated information systems must be subject to uniform and consistent approval processes. The default position is that PII are not to be exported, uploaded, or shared with a third party outside the college without such approval.

Requests to transfer PII outside the college are subject to the following procedure:

- The supervisor in the office seeking the data transfer will prepare a request that includes a detailed explanation of the purpose, the alternatives (if any) that have been considered, and the procedures that would be followed for transfer of and access to the data after the transfer.
- The office seeking the data transfer will obtain from the third party all available information about security procedures and contractual arrangements.
- The request is submitted to the convener of the Data Stewardship Committee*.
- The responsible person in the office requesting the data transfer should be prepared to meet with the Data Stewardship Committee to respond to questions and, if necessary, to obtain additional information from the third party that may be requested.
- When the Data Stewardship Committee has determined that it has all of the information that it needs, it will prepare a recommendation about the data transfer procedure. If deemed necessary, the Committee will refer questions to college counsel. (For example, there may be concerns of questions about indemnification requirements to address the question of liability should PII held by the third party be leaked either intentionally or accidentally.)
• The recommendation of the Data Stewardship Committee will be presented to the Executive Staff for discussion. If the recommendation is positive and no objection is raised, the request will be deemed to be approved. If the recommendation is negative or qualified, or if there are substantive objections raised in Executive Staff, this information will be sent to the original requester with an invitation to modify then request or appeal the decision directly to the Executive Staff.

Issues that will be addressed when considering a request for transfer of PII to third parties may include, but are not limited to, the following:

• The importance/urgency of the business need for the operations of the college (Because of the risks involved with third-party storage of college data, we should enter into these arrangements only when the function being addressed is compelling and more than a matter of convenience to the office involved.)
• The technical requirements for such data transfer, and the security of the procedures that are proposed for that transfer
• The legal restrictions applicable to the data proposed for transfer

In consideration of these three issues, the following questions will be asked:

✓ What is the level of risk (i.e., the severity of potential consequences) should data be released inappropriately?
✓ What chance is there that this data transfer will result in redundant data (e.g., multiple versions of addresses or other PII) that are not synchronized and, therefore, might cause operational confusion and error?
✓ What is the reputation and performance record of the third-party entity involved?
✓ What security measures are used by the third party to protect against deliberate or accidental release of college-owned data?
✓ What procedures are used by the third party for secondary (offsite) backup and storage of college-owned data?
✓ What procedures are proposed by the third party for long-term protection of our college data, including provisions for destruction of data when it is no longer needed or when the relationship with the College is terminated?
✓ What are the contractual agreements related to indemnification in the event of accidental or deliberate release of college data by third parties?

*As of April 2012, the members of this committee are: Richard Fass, Ken Pflueger, Andrew Crawford, Jennifer Rachford, Michael Denny.

Approved, April 2012