Our Collective Responsibilities for Protecting Personal Information

Lea Pennock and Rick Bunt

As our new administrative systems (such as AboutUS, SiRIUS, UniFi and PAWS) come on stream we are being asked many questions that relate to our collective responsibilities for safeguarding the personal information about our students, staff and faculty that resides in our databases. Our new systems did not create these issues, but they have raised some important questions about practices, processes and even policies. As we seek to provide answers to the questions coming our way there are a few distinctions we need to keep in mind, and some principles that should guide our use of personal information. New technology may change our processes, but our principles endure.

Ownership vs. Stewardship

Personal information (such as name, address and birthdate) belongs to the individual whose name, address and birthdate it is. Individuals do not relinquish ownership of this information by providing it to the University; rather, they entrust it to our use because they acknowledge that we need the information in order to provide services they want. As steward of this data, the University has certain obligations under law and our own regulations and policies (such as Council Regulations, the guidelines for academic conduct and the data use policy):

- the information is to be used only for the purposes for which it has been collected
- the information must not be shared with a third party without written consent
- the information must be destroyed when it is no longer needed
- those who have access to the information must understand their individual responsibilities and obligations

Much of the personal information that we collect about our students, faculty and staff is now held in electronic format in computer systems, but a great deal of it is also held in paper files, print-outs and other non-electronic formats. The same principles apply regardless of the format, and our policies, processes and practices must be developed accordingly.

Seeing Information vs. Using Information

Access to personal information does not necessarily confer the right to use it or divulge it. Employees have a responsibility to ensure that they do not make use of personal information to which they have been granted access unless they have a legitimate use for it in their role as an employee. A given employee may, moreover, be permitted to use a particular piece of information in one role but prohibited from using the same piece of information in another. For example, a faculty member may have access to a student's grades for advising purposes, but such access would not entitle her to use this information without the student's explicit permission were she considering hiring that student in her role as employer.

While technological solutions have the promise and potential for making it easier to control and monitor the extent to which information is available to a given employee, not all of that potential is yet realized. We continue to live within the limitations of our technology. Just as it is not always feasible to 'mask' information held in a paper file, so it is not always possible to hide certain fields displayed on computer screens. This doesn't change the underlying principles, however.

Institutional Responsibility vs. Individual Responsibility

As an institution, the University of Saskatchewan has certain responsibilities for ensuring that data is entered accurately, that it is held in secure systems, that appropriate approval processes are in place for its use and that its employees are aware of their legal and institutional responsibilities to safeguard the information and to use it responsibly. But these institutional safeguards are only part of the solution. Individual employees also have responsibility for understanding the purposes for which personal information has been provided and for using it accordingly. Inevitably, because of limitations in our technology, employees will have access to more information than they necessarily need to do their jobs. Their use of this information becomes a matter of trust and stewardship. We all have both collective and individual responsibilities as stewards of personal information.

For more information:

- U of S Guidelines for Academic Conduct: http://www.usask.ca/university_council/reports/guide_conduct.shtml
- The Local Authority Freedom of Information and Protection of Privacy Act: http://www.saskjustice.gov.sk.ca/legislation/ summaries/l_a_f_o_i_pact.shtml
- The U of S Data Use Policy: http://www.usask.ca/policies/4_38.htm

Lea Pennock is University Secretary and Rick Bunt is Associate Vice President, Information and Communications Technology.

October 13, 2005