BEST PRACTICES: ELECTRONIC POSTING OF STUDENT PERSONAL INFORMATION

I. INTRODUCTION

Under the *Freedom of Information and Protection of Privacy Act* (FIPPA) universities may collect and use the personal information necessary to deliver their programs. However, the Act also sets standards for handling this personal information. University faculty and staff are responsible for protecting students' right to privacy when handling their personal information and, in particular, protecting it from unauthorized access or disclosure. Students' personal information includes student grades, identification numbers, home phone numbers, personal e-mail addresses, and photos.

In light of this statutory obligation, University faculty and staff must exercise particular caution when posting student personal information electronically. Once posted, the University loses control of the information – it can be viewed by anyone with access to a computer (or access to a password protected site), and the information can be copied and manipulated. For this reason, for example, a composite class photo posted on the web without consent could lead to an allegation that the University had breached students' privacy rights and raise legitimate concerns about personal safety and security, while the same photo hanging in a School or Department corridor, while publicly available, would not give rise to similar privacy concerns.

"Electronic posting" includes the following:

- Uploading personal information to a publicly or widely accessible University webserver/website (individual, departmental, faculty/unit, or University-wide) including a password protected site accessible to faculty, staff and students in a particular program
- Uploading personal information to an external webserver/website (e.g., personal website, conference or journal site, collaboration space)
- Disclosing personal information through a blog, chatroom, online newsgroup, broadcast email, public email list, etc.

II. BEST PRACTICES FOR POSTING STUDENT INFORMATION ELECTRONICALLY

As a general best practice, Faculties, Departments, and individual faculty and staff should not post student personal information electronically without providing prior notice to the affected students and either giving them an opportunity to decline to have their personal information posted, or, in the case of particularly sensitive information, obtaining their written consent prior to the posting. There may be some cases where there is no need to obtain students' approval before posting their personal information so long as they have been given notice of the practice, but such situations will be relatively rare. For example, consent from intercollegiate athletes would not normally be required in order to post standard roster information, photos, and performance information and statistics on University websites.

Before posting student personal information, faculty and staff should ask themselves the following questions:

(i) Is the posting of student personal information necessary or desirable for the purposes of the particular program or activity?

(ii) If so, am I posting only the personal information that is necessary for those purposes and nothing more?

(iii) Have I provided sufficient notice to students regarding what information will be posted, why it will be posted, where it will be posted, and for how long it will be posted?

(iv) Have I given the students an opportunity to decline to have their personal information posted or obtained their written consent? (This will be necessary in most situations.)

III. RECOMMENDED BEST PRACTICES FOR SPECIFIC TYPES OF POSTINGS

1. STUDENT PHOTOS

Composite Class Photos
Avoid the electronic posting of composite class photos unless all students have received prior notice and each student has given written consent to the posting of his or her photo. The names and photos of students who have not consented should be removed before posting.

Individual or Group Photos
Avoid the electronic posting of individual or group photos of students, with or without identifying names, unless the students have received prior notice and have consented to the posting. While written consent is best, consent can be implied under certain circumstances (e.g., students showing up for a group photo shoot for graduate students after being told: (i) that participation was optional and (ii) where the photos will be posted).

Exception: It is not necessary to provide notice or obtain consent if student photos are posted solely for identification purposes on a secure site accessible only to those faculty and staff who need the photos for their academic or administrative responsibilities. Sufficient notice of this use is covered under the general collection notice in Western's academic calendars.

Candid Classroom/Lab Photos
Avoid the electronic posting of candid classroom or lab photos of students, with or without identifying names, unless students have been given prior notice and an opportunity to be excluded from the photo shoot.

Photos taken at Faculty / Department Social Events
The posting of individual or small group photos of attendees at Department and Faculty social functions or other events within a Faculty is of less concern than other types of postings. However, it is recommended that students (and others) attending such events be made aware that such photos may be posted electronically, and that any requests not to have a photo posted will be honored.

2. STUDENT NAMES, FACULTY AND PROGRAM

Western's official policy is that student name, Faculty of registration, and program of study are considered to be publicly available and are provided to third parties upon request*. However, the Policy also provides that students have the right to request that this information not be made public. Therefore, electronic posting of such information (e.g., lists of registered students posted on a Department or Program website) should be avoided unless students are made aware of the posting and have an opportunity to opt-out.
**Official Student Record Information Privacy Policy http://www.uwo.ca/univsec/handbook/general/privacy.pdf*

3. SCHOLARSHIP AND AWARD RECIPIENTS

Western's official policy is that information about academic or other University honors or distinctions received by a student is considered to be publicly available and is provided to third parties upon request*. However, the Policy also provides that students have the right to request that this information not be made public. Therefore, Faculties and Departments should not post such information electronically if they receive such a request.

**Official Student Record Information Privacy Policy http://www.uwo.ca/univsec/handbook/general/privacy.pdf*

Note: "Scholarship and Award Recipients" does not include recipients of needs-based awards and bursaries. Information on recipients of needs-based awards and bursaries should not be posted electronically.

4. STUDENT COURSE WORK

As a general rule, avoid posting details of individual students' academic work and activities on a website without prior notice and written consent. While there may be exceptions to the requirement for written consent if the University determines that the posting is a necessary part of a course or program, caution should be exercised. When in doubt, consult with Western's Privacy Office at privacy@uwo.ca.

Posting Marks

Do not post lists of student identification numbers and marks electronically. It is recommended that faculty and staff use WebCTVista when communicating marks electronically to students.

5. OTHER PERSONAL INFORMATION

As a general rule, avoid the electronic posting of other personal information such as students' home addresses, home telephone numbers, date of birth, educational history, extracurricular activities, and personal e-mail addresses without prior notice and written consent.

6. INFORMATION SECURITY

Appropriate information security controls should be in place for any system that stores or transmits student personal information. Contact your system administration group, check security.uwo.ca, or contact the Central Information Security Officer at its-ciso@uwo.ca for details about available and appropriate information security controls.