

CS Dept Policy in regard to Online Student Records

The spirit of this policy is to make sure that faculty and TAs do not expose private student information to the web and that private information is not exposed to other account holders on our network.

It is very important that the university policy, found in the faculty handbook section VI, Other Information, Student Record Policy (<http://www.odu.edu/ao/facultyhandbook/index.php>) be strictly followed in protecting students private information. If you save any students information on your computer, make sure you follow all guidelines as prescribed by the university (<http://occs.odu.edu/security/awareness/index.shtml>) in protecting this information.

Following are summary and detailed suggestions for how to conform to these directives for files on the Unix side. Similar procedures are available for files on the windows side that are potentially exposed through a web server.

Summary

Directory information can be published to the web - information such as name, address, e-mail; students can opt out from having even this information published

Protected information such as grades, GPA, university ID
can be used by faculty, TA, staff to perform duty such as grading
can only be given to individual student
should not be put into a public html directory (or subdirectory)
should not be world readable
no symbolic links to such information in public html directories
at least one directory containing a file with such information should be protected

TAs should not devise their own procedures for protection but follow one of the methods described below or consult with a faculty advisor.

Details

1)Directory Information: As defined by the University at <http://www.odu.edu/ao/registrar/about/policies/ferpa.shtml>, a selected set of information may be published as appropriate UNLESS the student has requested that it be kept confidential. Examples include the student's name, address, and email address. Directory information should not be published arbitrarily, but may be included in official documents with good cause.

Online directory information: TA's whose duties require dissemination of directory information should check with their faculty supervisor for a list of students in the related courses who have requested confidentiality.

Faculty and staff should honor requests for confidentiality as indicated in the student listings under LEO. Where the course design calls for publication of student work or projects, students who have requested confidentiality should be allowed to remove or request removal of all identifying information.

2) Protected Information: All information about a student that would go into students' records and that is not included in the University's list of directory information is protected. This includes, for example, individual student grades, GPA's and the University Identification Number.

Protected information may be USED by faculty, staff, TA's, etc. as required in the legitimate performance of their duties but should otherwise only be revealed to the individual student.

Online protected information: No files containing protected student information, in any format, should be placed in a public_html directory or any subdirectory thereof. There should be no symbolic links inside a public_html directory pointing outside that directory structure.

No files containing protected student information should be left in a world-readable state - one of the following must be true:

- 1) the file has protection 400 or 600
- 2) at least one of the directories containing it must be protected at the 400 or 600 level

If there are hard or symbolic links providing alternate paths by which a file may be reached, one of those two conditions must hold for every such path. Under direct instructions from a faculty member, files and directories may be assigned to restricted groups other than "student" and "grad" in which case a more relaxed level of group permission may be permitted.

All users of the CS Dept network are strongly urged to be sure that every file in their home directory that could possibly contain private information on students is readable only by them (permission 600) and that every subdirectory directly under their home directory that could contain files with such information, with the sole exception of public_html, is readable and executable only by them (permission 700).

TA's whose duties include providing protected information, such as grades, to students should consult with their faculty supervisor as to what protection mechanisms are available for disseminating such information. Under no circumstances should a TA simply post such information or attempt to devise their own means for disseminating protected information.