Storage, Access, and Transmission of Confidential and Personal Information Policy

Approved by Senior Administrators, December 11, 2007

Updated: December 09, 2010

Policy

It is the policy of Connecticut College to control access to and maintain the confidentiality of records that contain Personal Information, in order to protect the privacy of its students, faculty, and staff, to reduce the risk of identity theft, and to comply with relevant federal and state laws and regulations governing Personal Information, including:

- the Health Insurance Portability and Accountability Act of 1996 (HIPAA);
- the Family Educational Rights and Privacy Act of 1974 (FERPA);
- the Gramm-Leach-Bliley Act (GLB);
- Connecticut General Statutes §§ 42-470 and 42-471; and
- other state and federal statutes and regulations as appropriate.

To facilitate the protection of Personal Information collected, used, and/or maintained by Connecticut College, Connecticut College requires that its faculty and staff protect all confidential information, including Personal Information, by safeguarding it when in use, protecting it properly when not in use, and sharing it appropriately. Personal Information regarding other members of the college community will only be shared as allowed by state and federal law and college policy. As detailed in the Information Security Awareness for New Faculty and Staff Policy, all employees with access to Personal Information shall receive training at least once per year regarding the requirements of this policy.

For the purpose of this policy, "Personal Information" means:

i. information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number;
ii. protected health information as defined by HIPAA, which generally includes identifiable health information – with certain exceptions; and
iii. nonpublic personal information as defined by GLB.

Personal Information does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media. Personal Information includes information stored in any format, including but not limited to electronic media, hard copy documents, and certain types of information that may be conveyed orally. Any employee with questions about whether certain information constitutes Personal Information as defined by this policy or any other question about the meaning or implementation of this policy should contact the Office of the Vice President for Information Services.

Access to and disclosure of student education records that contain personally identifying information, as defined by FERPA, is governed by the College's FERPA policy, which is available from the Office of the Registrar and on-line at *http://www.conncoll.edu/cw40/c/document_library/get_file?p_l_id=10273&folderId=11802&name=DLFE-701.pdf* To the extent that student education records contain Personal Information as defined above, storage, access, transmission and disposal of such Information is governed by this policy as well.

Employees who do not comply with this policy may be subject to disciplinary action, including but not limited to, termination.

Procedures for Electronically Stored Personal Information

Storage of Personal Information in Electronic File:

1. All Connecticut College electronic files that contain Personal Information shall be stored on the central college servers or be encrypted and stored in a secure location. Such files may not be stored on personally-owned computers or devices.
2. All Connecticut College electronic files that contain Personal Information and that are stored on hard drives and storage devices being removed from service shall be completely erased and/or the devices destroyed.

Transmission of Personal Information in Electronic Files:

3. All off-campus connections to college servers that involve the transmission of Personal Information managed by Connecticut College must be through Banner Self-Service or through a secure VPN.
4. All Connecticut College files that contain Personal Information that are transmitted or transported off campus must be encrypted and must be stored on devices owned by Connecticut College.
5. All Connecticut College files that contain Personal Information shall not be transmitted over any public wireless network.

Access to Personal Information Contained in Electronic Files:

6. Employees may only access Personal Information contained in student records by contacting the Records and Registration Office. The Records and Registration Office will ensure that any access to student records is consistent with relevant law and Connecticut College policy.
7. Employees may only access Personal Information contained in employee records for any other employee by contacting Human Resources. Human Resources will ensure that any access to Personal Information contained in the employee record of another employee is consistent with relevant law and Connecticut College policy.

Procedures for Personal Information Stored in Hard Copy

Identification of Hard Copy Materials Containing Personal Information:

8. Employees should be aware of which hard copy materials contain Personal Information. Because Personal Information may appear in unusual or unconventional places, employees should review hard copy materials that they receive to determine whether or not the materials contain Personal Information.

Storage of Hard Copy Materials Containing Personal Information:

9. Employees must store hard copy materials with Personal Information in a locked cabinet. Any employee who has or, obtains hard copy materials with Personal Information, and who does not have a locked cabinet, should alert his or her supervisor.
10. When working with Personal Information in hard copy format, employees should take common sense precautions. For example, employees should not leave hard copy materials containing Personal Information on their desks when gone for a prolonged period of time, such as for lunch or overnight.
11. Each employee should only have, obtain, and keep the minimum amount of Personal Information necessary to perform his or her job. Similarly, employees should only copy and/or share hard copy materials containing Personal Information when it is necessary to perform the business of Connecticut College.

Transmission of Hard Copy Materials Containing Personal Information:

12. Employees may not take hard copy materials containing Personal Information off-campus without the permission and knowledge of their supervisor.
13. Any supervisor who permits an employee to take hard copy materials containing Personal Information off-campus must track the materials, including: (a) the Personal Information that has been taken off-campus; (b) the format of the materials; (c) the type of documents taken off-campus; (d) the purpose for which the material has been taken off-campus; (e) the time period for which the material is expected to be off-campus; and (f) that the materials have been returned. A supervisor must track this information in a written record, preferably by keeping a log.
14. Any supervisor who permits hard copy materials containing Personal Information to be taken off-campus must monitor the return of the materials in the agreed-upon time period. If the materials do not return in that agreed-upon time period, the supervisor must report the missing materials to the Office of the Vice President for Information Services within 24 hours. The ability of Connecticut College to investigate any potential loss of Personal Information critically depends on supervisors taking this requirement seriously.
15. Any employee who takes hard copy materials containing Personal Information off-campus must take common sense steps to protect that material. For example, employees should not leave the materials unattended, including in a bag in the

airport, in a locked but empty car, or in any other unattended location. Where possible, employees should keep hard copy materials containing Personal Information in their personal possession.

16. Any employee who takes hard copy materials containing Personal Information off-campus should take the minimum amount necessary to perform his or her job.
17. If practical, any employee who needs to take hard copy materials containing Personal Information off-campus should convert those hard copy materials into an electronic format and store the materials on an encrypted device.

Disposal of Hard Copy Materials Containing Personal Information:

18. Employees should dispose of hard copy materials containing Personal Information through the shredding services provided by Connecticut College. Employees may not dispose of hard copy materials containing Personal Information at home, while traveling, or by placing the materials in a trash bin. This means that employees who take hard copy materials containing Personal Information off-campus must return the materials to the College for disposal and not perform that disposal off-campus.
19. Each employee who has Personal Information in hard copy format must be aware of and comply with the Document Management Policy regarding the retention and destruction of different types of materials.