

TIDEWATER COMMUNITY COLLEGE
POLICY ON PERSONAL NON-PUBLIC INFORMATION

Purpose

This policy establishes requirements for protecting personal, non-public information (PNPI) and notifying individuals whose personal, non-public information may have been disclosed by computer security breaches or other means. The policy complies with the Virginia Government Data Collection and Dissemination Practices Act (Code of Virginia §2.2-3800) and certain Federal statutes, including the Family Educational Rights and Privacy Act (FERPA – educational records), Health Insurance Portability and Accountability Act (HIPAA – health information), and Gramm-Leach-Bliley Act (GLBA – financial institution and customer data).

Definition

Personal Non-Public Information (PNPI): any information that uniquely identifies a person and provides confidential information (e.g., academic, financial, medical records) about that individual. Social Security number, driver's license number, credit card and other financial account number in combination with name and security code or password needed to access the credit card or financial account pose a high risk of identity theft or financial loss to the individual if improperly disclosed. Personal, non-public information does not include published directory information or information that is lawfully made available to the general public from federal, state or local government records.

Policy

Tidewater Community College recognizes and respects the need for privacy of sensitive information, including PNPI. Maintaining the security of sensitive personal information is one of the college's most important responsibilities. TCC administrators, faculty, and staff with access to PNPI are held accountable for adhering to strict standards to prevent the misuse of sensitive information.

1. Employee access to PNPI is restricted to individuals on a "need to know" basis for the sole purpose of conducting the business of the college.
2. TCC emphasizes the importance of confidentiality and privacy through a combination of training, operating procedures, and systematically enforced information technology security.
3. TCC strictly adheres to FERPA, HIPAA, GLBA, Virginia law, and other relevant federal and state laws to protect the security of sensitive information.
4. TCC continually tests and updates its information technology resources to improve the protection of sensitive information residing on college servers.

**Policy on Personal
Non-Public Information
Page Two**

Unless required by law, or needed to perform core departmental activities that cannot be immediately facilitated by other means, Social Security numbers or other high-risk PNPI shall not be collected or stored.

Whenever possible, centrally administered information systems (e.g., VCCS Student Information System (SIS), Commonwealth Integrated Pay and Personnel System (CIPPS), etc.) must be used to retrieve, process, or store PNPI. PNPI will not be stored on college-owned local computing systems unless specifically authorized by the appropriate college vice president as defined in the companion college "Procedures for Protecting Personal Non-Public Information and Reporting Compromise of PNPI." Nor may reports or queries containing PNPI be downloaded from a centrally administered information system to a local computing system without specific authorization from the appropriate college vice president.

Data containing PNPI will not be transferred or downloaded to an employee's personal computing system. Nor will such data be transferred or downloaded to any portable storage media (e.g., disk, CD/DVD, USB drive, etc.). Exceptions to this aspect of this policy may be authorized only by the Vice President for Information Systems on the recommendation of the college vice president responsible for data.

Secure, encrypted communications must be used when collecting or transmitting PNPI. Personal, non-public information should not be sent via e-mail unless required by a government agency. Grades may be e-mailed only to a student's official VCCS e-mail address. Grades may not be e-mailed to a student's personal or other e-mail address nor from a faculty member's personal e-mail address.

At least annually, college departments must re-evaluate their acquisition, use, and safeguarding of PNPI for conformance to this policy and to the companion college procedure and Guidelines for Protecting Personal Non-Public Information.

Immediately following the discovery of a breach in the security of a system in which PNPI may have been accessible, appropriate action will be taken by the responsible college vice president to assess the likelihood that PNPI may have been compromised and to notify all persons whose personal information might have been compromised. This provision applies whether the system in which the data was stored was paper- or computer-based. A computer security breach is any incident in which the security of a computer system is compromised, including theft or loss of a computer or storage device or medium where unauthorized person(s) might have been able to access, copy, or read data files on it. It does not include normal business use by authorized employees or third-party business partners of the college authorized to receive and process PNPI collected by the college.

Implementation

The Vice President for Administration shall be responsible for developing and maintaining procedures that are consistent with this policy and that comply with

**Policy on Personal
Non-Public Information
Page Three**

applicable policies and procedures of the Virginia Community College System and the Commonwealth of Virginia.

Authorization: Deborah M. DiCroce, President

Date: July 13, 2006

Effective Date: Immediately