Chapter 5 – Student Services

AP 5800 PREVENTING IDENTITY THEFT IN STUDENT FINANCIAL TRANSACTIONS

References:

15 U.S. Code Section 1681m(e) (Fair and Accurate Credit Transactions Act)

These procedures shall be administered by the Vice President of Administrative Services or designee and the Vice President of Student Support Services or designee depending on the administrative unit responsible for the student financial transaction.

Definitions:

"Identity Theft Prevention Program" (ITPP) is a program designed to prevent identity theft in student financial transactions.

"Identity theft" is a fraud attempted or committed using identifying information of another person without authority.

A "creditor" includes government entities who defer payment for goods or services (for example, payment plans for enrollment fees, bookstore accounts, parking tickets, etc.), issued loans or issued student debit cards. Government entities that defer payment for services provided are not

"Red" means any individual who is receiving goods, receives a loan, and/or is issued a debit card from the District and is making payments on a deferred basis for said goods, loan, and/or debit card.

"Identifying information" means any name or number that may be used alone, or in conjunction with any other information, to identify a specific person including, but not limited to, name, social security number, ethnicity, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, bank account number, bank routing number, credit card number, credit card expiration date, card holder name or address, pay rate, direct deposit information, or student identification number.

Purpose - The purpose of the Identity Theft Prevention Program (ITPP) is to control reasonably foreseeable risks to students from identity theft in student financial transactions, by providing for the identification, detection, and response to patterns, practices, or specific activities ("Red Flags") that could indicate identity theft.

District or campus shredding device. District records, however, may only be destroyed in accordance with State of California laws and regulations and consistent with the Districts' records retention policy.

F. Sensitive information is never to be taken from the work area without the approval of the supervisor.

G. Sensitive information being scanned into the District's laser fiche database or other electronic information storage system must be immediately returned to a secure location or shredded when scanning is complete.

H. When printing documents with sensitive information, to a common area, pick them up immediately.

[illegible] - Each employee and contractor performing work for the District will comply with the following policies:

A. Internally, sensitive information may be transmitted using approved District e-mail. All sensitive information must be encrypted when stored in an electronic format.

B. Any sensitive information sent externally must be encrypted and password protected and only to approved recipients.

b.

(1) Documents provided for identification appear to have been forged or altered.

(2)

(b) A material change in electronic fund transfer patterns in connection with a payment.

(3) A covered account that has been inactive for a reasonably lengthy period of time is suddenly used or active.

(4) Mail sent to the person holding the covered account is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the person's covered account.

(5) The District is notified that the person is not receiving paper account statements.

(6) The District is notified of unauthorized transactions in connection with a person's covered account.

(7) The District becomes aware of an electronic data security breach relating to a specific covered account.

e. [illegible]

and in the course of business, provides information to the credit reporting agency; or

10. Determine that no response is warranted under the particular circumstances.

Updating the ITPP

A. The District shall review and revise as needed this ITPP on an annual basis to reflect changes in risks to persons with covered accounts, and/or to reflect changes in risks to the safety and soundness of the District from identity theft, based on the following factors:

1. The experiences of the District with identity theft;

2. Changes in methods of identity theft;

3. Changes in methods to detect, prevent, and mitigate identity theft;

4. Changes in the types of covered accounts that the District maintains;

5. Changes in the business arrangements of the District, including service provider arrangements.

Staff Training

A. Staff training shall be conducted through the District's staff development program for all employees and officials for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the District or its customers.

B. Enrollment Services, Financial Aid, EOPS, and Veterans Affairs or designee is responsible for identifying employees and contractors related to their administrative unit requiring training in the ITPP program. The Director of Fiscal Services or designee is responsible for identifying employees and contractors related to their administrative unit requiring training in the ITPP program.

C. These employees or contractors must receive annual training in all elements of this policy when changes occur.

D. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the District's administrative regulations are made.

Oversight of Service Provider Arrangements