BP 3730 PRIVACY PROTECTION

The District collects and maintains confidential information relating to its students, employees, and individuals associated with the District, and is dedicated to ensuring the privacy and proper management of this information. The District is committed to actively ensuring that necessary procedures and awareness exists for District employees and students to comply with both the letter and the spirit of the Family Educational Rights and Privacy Act (FERPA) of 1974. The District is committed to increasing awareness of the confidential nature of social security numbers; reducing reliance upon social security numbers for identification purposes; developing consistent procedures regarding the use of social security numbers throughout the District; and assuring students and employees that social security numbers are maintained in a confidential manner.

Also see BP/AP 5040 titled Student Records, Directory Information, and Privacy

References: Family Educational Rights and Privacy Act (FERPA) 1974 (20 U.S. Code Section 1232g and 34 Code of Federal Regulations Part 99); Civil Code Section 1798.85

Adopted: 8/21/07
Revised: 1/10/17

(Replaces Board Policy 8996)
AP 3730 PRIVACY PROTECTION

It is the responsibility of all District employees to maintain and safeguard confidential information belonging to students, employees, applicants for employment, and individuals associated with the District. Per Civil Code Section 1798.85, state and federal law allows for the collection, use, and release of social security numbers. In addition, state and federal law does allow the use of social security numbers for internal verification and administrative purposes if it has been consistently used in that manner. To ensure privacy and avoid misuse of social security numbers, the following guidelines have been established regarding the use of social security numbers.

Guidelines

1) Each department’s administrator has responsibility for overseeing social security number usage in his/her department.
2) All departments will rely on the current student identification number system for identification and authentication of students for services.
3) Grades and other pieces of personal information will not be publicly posted or displayed in a manner where the social security number identifies the individual associated with the information.
4) All District forms and documents will remove social security numbers if not required.
5) In some situations, social security numbers will be released by the District to entities outside the District only as allowed by law, or when permission is granted by the individual; or when the external entity is acting as the District’s contractor or agent and adequate security measures are in place to prevent unauthorized dissemination to third parties; or when legal counsel has approved the release.
6) The social security number may continue to be stored as a confidential attribute associated with an individual. The social security number will be used as allowed by law.
7) In order to ensure confidentiality and to reduce the risk of social security unauthorized disclosure, District employees will use care and judgment, based on a respect for individual privacy and concern for the District’s interests.
   a) Do not leave paper documents containing confidential information unattended; protect them from the view of passers-by or office visitors.
b) Do not leave the keys to file drawers containing confidential information in unlocked desk drawers or other areas accessible to unauthorized staff.

c) Paper documents that contain confidential information critical to the conduct of District business must be stored in a secure location.

d) Shred confidential paper documents that are no longer needed, and secure such documents until shredding occurs.

e) Immediately retrieve or secure sensitive documents that are printed on copy machines, fax machines, and printers.

f) Double-check fax messages containing confidential information:
   i. Recheck the recipient's number before you hit send.
   ii. Verify the security arrangements for a fax's receipt prior to sending.
   iii. Verify that you are the intended recipient of faxes received on your machine.
   iv. Refrain from storing personal copies of information containing social security numbers in accessible places.
   v. Report all theft of confidential data immediately to Allan Hancock College Police Department.

g) Do not remove paper documents or electronic files containing confidential information from the District premises.

Also see BP/AP 5040 titled Student Records, Directory Information, and Privacy

References: Family Educational Rights and Privacy Act (FERPA) 1974 (20 U.S. Code Section 1232g and 34 Code of Federal Regulations Part 99); Civil Code Section 1798.85

Approved: 8/21/07
Revised: 12/13/16
(Replaces Administrative Procedure 8996.01)