Title	Policy ID:	
VSC Information Sensitivity Policy	**627-1**	
	Version: **2.0**	Date: **2018/12/14**

1. Purpose

1.1. The Information Sensitivity Policy is intended to help employees determine the level of care to use when disclosing information inside and outside of the VSC, as well as methods to be used for distributing, storing, and disposing of this information.

2. Scope

2.1. The information covered in this policy includes, but is not limited to, administrative information that is stored or shared by any means. This includes:

- electronic information
- written information on paper
- Information shared orally or visually (such as over the telephone or videoconferencing).

3. Policy

3.1. All VSC administrative information is categorized as Public or Protected information. In all cases, VSC information is presumed to be protected unless expressly designated as public under this policy.

3.2. Data ownership for the purposes of this policy resides at the VSC college or entity originating the data; unauthorized use of student or employee data from another VSC college or entity is prohibited. Data owner is defined as the person or department responsible for originating the data.

3.3. Public Information

Public information is information that the VSC makes available through its publications or public information site and other information that is considered a public record in accordance with state and federal law.

Examples of public information:

- Employee name, salary, department, title, and employment dates for employment verification and references.

Student directory information: the VSC FERPA policy has defined directory information as "information which would not generally be considered harmful to the student or an invasion of privacy, if disclosed." Directory Information is defined by each school.

Note: Students may opt out of the release of all of this information annually by completing a student privacy restriction request; in such cases, the information becomes classified as protected. Directory information should not be released until a determination has been made that the student has not opted out of release. While directory information may be made public, a college may, at its discretion, elect not to disclose such information.

Public data may be accessed by VSC employees, students, and external constituents. Requests for information will be referred to the data owner. Some requests may need to be confirmed in writing; public data will not necessarily be publicly disseminated without formal approval.

3.4. Protected Information

Protected information at the VSC is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information." (Definition of PII from NIST 800-122) It is all information protected by FERPA, the Vermont Public Records Act or other legal provisions. Any information not discretely listed as Public information above, it should be considered protected information.

Protected information cannot be distributed outside of the VSC without approval. Certain protected information may be distributed within the VSC, if permitted by state or federal law or this policy. The guidelines for distribution vary according to the type of information, the degree of risk associated with it, the internal recipient(s), and any applicable state and federal law, such as FERPA or HIPPA.

VSC employees are encouraged to use common sense and good judgment in properly securing all information. For example, telephone conversations are generally regarded as not secure. However, the VSC recognizes the need to discuss protected data over the phone. Employees engaging in private telephone conversations should take measures such as closing an office door and using the Colleague ID number. Authentication in relation to personally identifiable information should be in accordance with FERPA. If you are unsure about how to handle a particular piece of information, you should contact your supervisor.

Examples of data considered to be protected is below. This is not a comprehensive list.

- Colleague ID
- VSC username
- Admission reports
- Class rosters
- Employee and student resumes
- Student portfolios

- Financial aid awards
- Employee benefits
- Inter-collegiate athletic eligibility
- Vendor contracts that are determined to include proprietary information
- Employee home address and phone number unless printed with permission
- Calendar appointments
- Social Security number
- Ethnicity
- Race
- Nationality
- Name of parent or other family members
- Directory information for students who have opted out of public disclosure
- Academic standing and grades
- Payroll transactions
- Data from security audits
- Technical code purchased from vendors
- Information about groups of students or employees
- Passwords
- Credit-card holder data
- Employee and student applicant information
- Personal financial, medical or counseling information and personnel information protected by law

Protected data should only be accessed by authorized VSC personnel with a legitimate employment or educational need to know. Requests to distribute data should refer to the data owner. Requests need to be confirmed in writing, documenting contact information for the requester, the extent of the information requested, and the use of the information requested.

3.5. Accountability/Enforcement

3.5.1. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Any disciplinary action considered in association with a critical incident shall follow procedures set forth in the relevant employee collective bargaining agreement or, in the case of employees not covered by a collective bargaining agreement, the VSC personnel handbook.

4. References

VSC Records Retention Policy
VSC Policy 312 – Guidelines for Compliance with the Family Educational Rights and Privacy Act (FERPA)
9 V.S.A. Chapter 62 – An Act Relating to the Protection of Personal Information
1 V.S.A. § 317 – Vermont Public Records Law
NIST 800-122

5. Definitions

5.1. VSC – Vermont State Colleges

6. Revisions

Date	Revision	Approval	Signature
09/20/07	Approved	Council of Presidents	
May 7, 2009	Amended		
April 17, 2012	Amended		
2018/10/16	Approved	IT Council	IT Council
2018/12/17	Approved	CIO - Kevin Conroy	Kevin Conroy