VSC Information Sensitivity Policy

1.0 Purpose

The Information Sensitivity Policy is intended to help employees determine what information can be disclosed within and outside of the VSC, as well as the methods to be used for distributing, storing, and disposing of this information.

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

All faculty and staff should familiarize themselves with this information handling policy. It provides prudent steps that you should take to protect private information.

Questions about a specific piece of information and non-technical issues should be addressed to your supervisor. Technical questions about safeguarding information and secure transmission methods should be directed to local IT.

2.0 Scope

All VSC administrative information is categorized as:

- Public, or
- Private

3.0 Public Information

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

Data ownership for the purposes of this section 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.

Examples of public information:

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

- Data included on the VSC Public Information Tab of the Blackboard portal.
- 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." For the purposes of this policy, directory information includes the following:
  - Name
  - Home and college address
  - Telephone listing
  - Email address
  - Date of birth
  - Major
  - Enrollment status (full-time or part-time)
  - Enrollment level (undergraduate or graduate)
  - Dates of attendance
  - Degrees and awards received
  - Weight and height of athletic team members
  - Photographs
  - Most recent and previous educational institutions attended
  - Participation in officially recognized activities and sports

  Note: Students may opt out of the release of part or all of this information annually by completing a student privacy restriction request; in such cases, the information becomes classified as private-privileged. 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.

Access: VSC employees, students, and external constituents

Responding to requests: Refer requests to the data owner. Some requests may need to be confirmed in writing; public data will not necessarily be publicly disseminated without formal approval.

Distribution within VSC: Portal, email, interoffice mail, telephone, electronic transmission methods

Distribution outside of VSC: Portal, email, U.S. mail, telephone, electronic transmission methods

Storage: Unrestricted, unless protected by FERPA.

Disposal/Destruction: Will follow the VSC Records Retention policy.

4.0 Private Information

Private information is all information protected by FERPA, the Vermont Public Records Act or other legal provisions.

Private information cannot be distributed outside of the VSC without approval. Certain private 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. In all cases, VSC information is **presumed to be private** unless expressly designated as public under this policy.

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 private 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.

Data ownership for the purposes of this section 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.

Policy

These classifications provide details on how to protect private information.

Private-Restricted: Employee, student, and institutional information not considered public; would pose a low-to-medium threat if accessed by a third party without proper authorization.

Examples:

- 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

Access: Authorized personnel with a legitimate employment or educational need to know. Responding to requests to distribute within the VSC: Refer requests to the data owner.

Responding to requests to distribute outside of VSC: Refer requests to the data owner.

Distribution within VSC: Only for authorized VSC personnel through telephone conversations; VSC-supplied unencrypted e-mail; paper documents. Paper documents should be placed in an envelope or folder.

Distribution outside of VSC: To individuals or entities if authorized, permitted or required by law, using VSC-supplied and IT-approved secure transmission methods, US mail and telephone. In all cases, steps will be taken to verify the credentials of the requestor before distributing any data.

Storage: Follow the VSC Data Access Security Policy and the VSC Records Retention Policy as applicable.

Disposal/Destruction: Follow the VSC Records Retention Policy.

Private - Privileged: Student and personnel information; some information about the organization; would pose a medium-to-high threat if accessed without proper authorization. Includes non-directory student data, personnel information, data restricted under third party non-disclosure agreements, data related to security and infrastructure; information related to employee or student discipline.

Examples:

- 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
- Private-restricted 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

Access: Authorized personnel with a legitimate employment or educational need to know.

Responding to requests to distribute within the VSC: Refer requests to the data owner. Some requests may need to be confirmed in writing.

Responding to requests to distribute outside of VSC: Refer requests to the data owner. Requests need to be confirmed in writing.

Distribution within VSC: Only for authorized VSC personnel through VSC-supplied and IT-approved secure transmission methods; telephone conversations; paper documents. Paper documents should be marked confidential and placed in an envelope or folder.

Distribution outside of VSC: To approved business partners who have met VSC third party security requirements, or to individuals or entities if authorized, permitted or required by law, using VSC-supplied and IT-approved secure transmission methods, or by telephone. Except for private-privileged information required by law or external business processes to be distributed to individuals or organizations (e.g., W-2's, 1099's, 1098's, wage garnishments, employment verifications), paper distribution should be marked confidential and sent via registered mail with signature confirmation. In all cases, steps will be taken to verify the credentials of the requestor before distributing any data.

Storage: Follow the VSC Data Access Security Policy and the VSC Records Retention Policy as applicable.

Disposal/Destruction: Follow the VSC Records Retention Policy.

5.0 Accountability/Enforcement

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.

6.0 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

Approved by/on: Council of Presidents, 09/20/07
Amended: May 7, 2009; April 17, 2012