SNOW COLLEGE

Policy # 12.1
Date Approved: 5-18-2000
Date Amended: 1-27-2017
Responsible Office: Information Security

SUBJECT: INFORMATION TECHNOLOGY ACCEPTABLE USE POLICY

1.0 GENERAL STATEMENT

1.1. Snow College makes available to its community members technology resources, including email and internet, to support the educational, instructional and administrative activities of Snow College. These resources are to be used to advance the mission of the College. These resources are to be used in a manner consistent with College Policy, Law and Rules. Every user bears the responsibility for knowing and complying with applicable Policy, Laws, and Rules; for appropriately securing their computers and other electronic devices from misuse or theft by others; and for avoiding any use that interferes with others' legitimate access to and use of College Technology Resources.

2 TERMS

2.1. "User" or "Users" are the students, faculty, staff and authorized visitors, guests, affiliates and others to whom Technology Resources are made available.

2.2. "Technology Resources" are the College owned devices and systems, College contracted systems and services, and privately owned or publicly provided devices using the College's networks and resources. Included are College owned facilities such as computer hardware, multimedia hardware, video equipment, software, documentation, communications support, on-line account administration, support services, Internet access and instructional materials.

2.3. "Policy, Law and Rules" includes this Policy, the Information Security Policy, Technology Resource Guidelines, specialized policies created by specific departments, programs and offices of the College, and federal and state laws and rules including copyright laws.

2.4. "Electronic Messages or Traffic" includes emails, texts, voicemails, instant messages, internet use and other electronic communications transmitted sent or received using College Technology Resources.

3 Applicability.

3.1. This Policy applies to all Users and all technology administered within the College Internet domain by individual departments or members of the faculty or staff or by campus organizations, to information services hosted by dorm-resident students or by authorized resident visitors on their own hardware

connected to the campus network; to the resources administered by central administrative departments such as the College Library or IT; to authorized collaborative devices connected to the campus network and using College Internet addresses; to personally-owned devices connected by wire or wireless service to the campus network from College owned housing or via campus locations providing mobile wired access or wireless access; and to actions originating from computer systems or mobile devices maintained or used by members of the campus community off-campus but connecting remotely to the College's network services and under the aegis of the College's name. It applies to websites bearing the College credentials, even when hosted outside the College's Internet domain.

4 POLICY

4.1. Acceptable Use. Use of all College Technology Resources, information technology and digital resources should be for purposes that are consistent with the College's educational mission and the Policy, Law and Rules (including license agreements and terms of service) of the College, and not for commercial purposes.

4.2. Personal Use. Users may also use College Technology Resources for appropriate incidental personal use so long as those activities are legal and do not violate College policies; contractual obligations; the safety, security, privacy, reputational and intellectual property rights of others; or other restrictions.

4.3. Prohibited Use. Use of the College's Technology Resources should not violate applicable Policy, Law and Rules and may not be used to transmit malicious, harassing or defamatory content.

4.4. Use Is A Privilege And May Be Revoked. The use of the College Technology Resources, including networking and the internet, is a privilege, not a right. Inappropriate use, including any violation of Policy, Law and Rules, may result in cancellation of the privilege.

4.5. College Access.

4.5.1. College Access To All Use Of Technology Resources. In the event the College has reasonable suspicion that a User has violated any civil or criminal law, the College Code of Conduct, this Policy, or any other Policy, Law and Rule, the College reserves the right to

and the User agrees that the College may monitor, access, inspect, remove, copy, take possession of, or surrender to civil or criminal authorities the offending Content, with or without notice or consent of the User. The includes monitoring and accessing Electronic Messages or Traffic. Further, the College may monitor the Technology Resources to ensure that they are secure and being used in conformity with this Policy, Law and Rule. Information that the College gathers from such permissible monitoring or examinations may also be used in disciplinary actions.

4.5.2. College Access To Employee Generated Content. Employees are notified that the College owns all data and files in any computer, network, or other information system used by the College and to all data and files sent or received by employees using any College Technology Resources. This includes Electronic Messages or Traffic sent or received using College Technology Resources. The above are not private or confidential, and are the property of the College, and may be accessed or monitored as determined by the College.

4.6. Violations of this Policy may result in disciplinary action, including dismissal from employment, expulsion from the College, suspension or termination of Technology Resources use and privileges.

4.7. Utilization of any College Technology Resources constitutes acceptance of the terms of this Policy. Users acknowledge they have read and understand this Policy and they shall be personally responsible for their acts or omissions in connection with utilization in derogation of this policy.

4.8. Guidelines. The Snow College Office of Information Technology may from time to time publish and update "Guidelines To The Information Technology Acceptable Use Policy." Such Guidelines are binding upon Users.

4.9. The College makes no warranties of any kind, whether expressed or implied, for the services it provides, in connection with the use of the Internet. The College will not be responsible for any damages an employee or other user

suffers. This includes loss of data resulting from delays, non-deliveries, or service interruptions caused by the College's negligence, by the user's errors or omissions or by any other cause. Use of any information obtained via the Internet is at the user's own risk. The College specifically denies any responsibility for the accuracy or quality of information obtained through this service. All users need to consider the source of any information they obtain, and evaluate how valid that information may be.

4.10. Unauthorized uses of the College information technology facilities include, but are not limited to:

- Any utilization infringing on the rights or liberties of another.
- Illegal or criminal use of any kind.
- Utilization involving communications, material, information, data or images prohibited by legal authority as obscene, pornographic, threatening, abusive, harassing, discriminatory, or in violation of any other College policies.
- Deliberately wasting or overloading computing resources.
- Accessing, viewing, printing, storing, transmitting, disseminating or selling any information protected by law or subject to privilege or an expectation of privacy.
- Utilization that causes or permits materials protected by copyright, trademark, service mark, tradename, trade secret, confidential or proprietary data and information statutes, or communications of another to be uploaded to a computer or information system, published, broadcast, or in any way disseminated without authorization of the owner.
- Use of electronic communication systems to create or transmit unsolicited bulk messages (commonly known as 'spam'), content intended for commercial gain, or content which violates applicable state or federal laws.
- Any attempts to access any resources, features, contents, or controls of the information technology facilities that are restricted, confidential or privileged.
- Intentional or reckless utilization of resources causing damage to or altering the operation, function or design of the information technology

facilities or content.

- Granting access to persons not authorized by the College to any College information facility, either by intentional action such as disclosure of account information or unintentional action such as failure to log off.
- Commercial, profit-motivated or partisan political use not related to College programs.
- Any violation of applicable school policy or public law by such use.
- Any activity that is contrary to the high moral standards which must be maintained in an educational setting.
- The transmission to others of profane, defaming, harassing or offensive language.
- Any commercial use, product advertisement or improper promotion of political candidates.
- Any attempt to disrupt or interfere with use of the Internet system.
- Any attempt to access improper information to which the account holder does not have right to access.

1.8 Vandalism is defined as any malicious attempt to harm, modify, or destroy data of another user, the College data systems, Internet, or other networks. This includes, but is not limited to, the uploading or creating of computer viruses. Harassment is defined as the persistent annoyance of another user, or the interference of another users' work. Harassment includes, but is not limited to, the sending of unwanted mail. Vandalism and harassment may result in cancellation of user privileges and possible disciplinary action.

1.9 Security on any computer system is a high priority, especially when the system involves many users. Users must never allow others to use their password. Users should protect their password to ensure system security and their own privilege and ability to continue to use the system. The College is not responsible for individual password security.

- If you identify or suspect a security problem on the Internet, you must notify a system administrator. Do not demonstrate the problem to other users.
- Do not use another individual's account without express written permission of the account holder and system administrator.

- Any user identified as a security risk for having a history of problems with other computer systems may be denied access to the Internet by the College.

1.10 Due to the inherent lack of security in most Internet communications, and due to the right and need for the College to monitor compliance with civil or criminal law, the College Code of Conduct, the IT Acceptable Use Policy, or any other College policy, procedure, or regulation, any user utilizing any College information technology facility understands and agrees they are specifically waiving any expectation or right to privacy in their communications, data, programs, or other personal information stored, displayed, accessed, communicated, published or transmitted on the facilities.

SNOW COLLEGE

Policy #12.2
Date Approved: 12-18-2003
Date Amended: 1-27-2017
Responsible Office: Information Security

SUBJECT: DATA CLASSIFICATION AND HANDLING POLICY

1.0 PURPOSE

The purpose of this policy is to establish a framework for classifying and handling college data based on its level of sensitivity, value and criticality to the college as required by the College's information security plan. Classification of data will determine the baseline security controls for the protection of data. This policy applies to all College employees who access, process, or store sensitive College data.

2.0 DEFINITIONS

2.1. *Personally Identifiable Information (PII).* Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on Snow College interests, the conduct of College programs or the privacy to which individuals are entitled. Examples of such data would include that data protected by the Government Records Access and Management Act (GRAMA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) or other laws governing the use of data or data that has been deemed by the College as requiring protective measures. Also included in this class of information are Credit Card and Social Security numbers.

2.2. *Data Owner.* An individual or group of people who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit of the College.

2.3. *Data Custodian.* Employee of the college who has administrative and/or operational responsibility over information assets.

2.4. *Institutional Data.* All data owned or licensed by the College.

2.5. *Information Assets.* Definable pieces of information in any form, recorded or stored on any media that is recognized as "valuable" to the college

2.6. *Non-public Information.* Any information that is classified as Internal/Private Information according to the data classification scheme defined in this document.

3.0 POLICY

3.1. Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the College should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All institutional data should be classified into one of three sensitivity levels (tiers), or classifications:

3.1.1. **Personally Identifiable Information (PII).** Data is classified as PII when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the College or its affiliates. Examples of PII data include data protected by state or federal privacy regulations and data protected by confidentiality agreements. The highest level of security controls should be applied. Access to PII data must be controlled from creation to destruction, and will be granted only to those persons affiliated with the college who require such access in order to perform their job "need-to-know". Access to PII data must be individually requested and then authorized by the Data Custodian who is responsible for the data. PII data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law. In addition, the negative impact on the institution should this data be incorrect, improperly disclosed, or not available when needed is typically very high. Examples of PII data include official student grades and financial aid data, social security and credit card numbers, and individuals' health information.

3.1.2. **Internal Data.** Data is classified as Internal when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the College or its affiliates. By default, all information assets that are not explicitly classified as PII or public data should be treated as internal data. A reasonable level of security controls should be applied to internal data.

Access to Internal data must be requested from, and authorized by, the data owner who is responsible for the data. Access to internal data may be authorized to groups of persons by their job classification or responsibilities "role-based" access, and may also be limited by one's department.

Internal data is moderately sensitive in nature. Often, internal data is used for making decisions, and therefore it's important this information remain timely and accurate. The risk for negative impact on the College should this information not be available when needed is typically moderate. Examples of internal data include official College records such as financial reports, human resources information, some research data, and budget information.

3.1.3. **Public Data.** Data is classified as public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the College and its affiliates. While little or no controls are required to protect the confidentiality of public data, some level of

control is required to prevent unauthorized modification or destruction of public data. Public data is not considered sensitive; therefore, it may be granted to any requester or published with no restrictions. The integrity of public data should be protected. The appropriate data owner must authorize replication or copying of the data in order to ensure it remains accurate over time. The impact on the institution should public data not be available is typically low (inconvenient but not debilitating). Examples of public data include directory information, course information and research publications.

3.2. Determining Classification

3.2.1. The goal of information security, as stated in the College's Information Security Policy, is to protect the confidentiality, integrity and availability of information assets and systems. Data classification reflects the level of impact to the College if confidentiality, integrity or availability of the data is compromised.

3.3. Data Handling Requirements

3.3.1. For each classification, several data handling requirements are defined to appropriately safeguard the information. It's important to understand that overall sensitivity of institutional data encompasses not only its confidentiality but also the need for integrity and availability.

3.3.2. The attached table defines required safeguards for protecting data and data collections based on their classification. In addition to the following data security standards, any data covered by federal or state laws or regulations or contractual agreements must meet the security requirements defined by those laws, regulations, or contracts.

3.3.3. Predefined Types of PII Information Assets. Based upon state, federal, and contractual requirements that Snow College is bound by, the following information assets have been predefined as PII data and must be protected.

3.3.4. Personally Identifiable Education Records. Covered under FERPA.

Personally Identifiable Education Records are defined as any education records that contain one or more of the following personal identifiers:

- Student Badger ID Number
- Grades, GPA, Credits Enrolled
- Social Security Number
- A list of personal characteristics or any other information that would make the student's identity easily traceable

3.3.5. Personally Identifiable Financial Information(PIFI). Covered under GLBA. For the purpose of meeting security breach notification requirements, PII is defined as a person's first name or first initial and last name in combination with one or more of the following data elements:

- Social security number
- State-issued driver's license number
- Date of Birth
- Financial account number in combination with a security code, access code or password that would permit access to the account

3.3.6. Payment Card Information. Covered under PCI DSS. Payment card information is defined as a credit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

- Cardholder name
- Service code
- Expiration date
- CVC2, CVV2 or CID value
- PIN or PIN block
- Contents of a credit card's magnetic stripe
- Contents of Card Chip

3.3.7. Protected Health Information (PHI). Covered under HIPAA. PHI is defined as any individually identifiable information that is stored by a covered entity, and related to one or more of the following:

- Past, present or future physical or mental health condition of an individual.
- Provision of health care to an individual.
- Past, present or future payment for the provision of health care to an individual
- PHI is considered individually identifiable if it contains one or more of the following identifiers:
    - Name
    - Address (all geographic subdivisions smaller than state including street address, city, county, precinct or zip code)
    - All elements of dates (except year) related to an individual including birth date, admissions date, discharge date, date of death and exact age if over 89
    - Telephone/Fax numbers
    - Electronic mail addresses
    - Social security numbers

- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate number
- Device identifiers and serial numbers
- Universal Resource Locators (URLs)
- Internet protocol (IP) addresses
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number or characteristic that could identify an individual

- If the health information does not contain one of the above referenced identifiers and there is no reasonable basis to believe that the information can be used to identify an individual, it is not considered individually identifiable and; as a result, would not be considered PHI.

4.0 REFERENCES

12.4 Information Security Policy

12.5 Information Technology Acceptable Use Policy

Classification	Definition	Access Restrictions	Transmission	Storage	Disposal
Public	Information deemed to be public by legislation or policy. Information is in the public domain. Examples include annual reports, public announcements, the telephone directory, and specific categories of employee and student information.	No restrictions on access.	No special handling required.	No special safeguards required.	Media can be recycled.
Internal Use	Information not approved for general circulation outside the College. Loss would inconvenience the College or management; disclosure is unlikely to result in financial loss or serious damage to credibility. Examples include internal memos, minutes of meetings, internal project reports.	Access limited to employees and other authorized users.	No special handling required.	Access controlled by physical (locks) or electronic (passwords) safeguards.	Shredded or erased media.
Personally Identifiable Information (PII)	Information that is available only to authorized persons. Loss could seriously impede the College's operations; disclosure could have a significant financial impact or cause damage to the College's reputation. Examples include specific categories of employee and student information, unit budgets, accounting information, and information protected by legal privilege.	Access limited to those with a demonstrated need to know and official approval.	Encryption mandatory for public networks. Encryption optional for internal networks.	Access controlled by physical (locks) or electronic (passwords or two-factor authentication) safeguards	Shredded, degaussed or destroyed.

SNOW COLLEGE

Policy # 12.4
Date Approved:
Date Amended: 1-27-2017
Responsible Office: Information Security

SUBJECT: INFORMATION SECURITY POLICY

1.0 SUMMARY

1.1. The Snow College Information Security Policy ("Policy") applies to all organizations within the College, although the data needed and used by those organizations are different. Additionally, all College owned devices including, but not limited to workstations, lab computers, and kiosks are affected by this Policy unless otherwise stated. **The principles of academic freedom and free exchange of ideas apply to this Policy, which is not intended to limit or restrict those principles.** This policy is intended to be in accordance with federal and state laws and regulations regarding information security.

1.2. Each organization within the College must appropriately apply this policy to make certain they are meeting the requirements regarding Information Security. It is recognized that the technology at some organizations may limit immediate compliance with the policy; such instances of non-compliance must be reviewed and approved by the Information Security Office (ISO) and the Information Security Advisory Council (ISAC). Reference Section 4.19 for more information about policy exceptions.

1.3. College information technology resources are a valuable college asset and must be managed accordingly to assure their integrity, security, and availability for lawful educational purposes. This document describes the policy for use by all persons and/or organizations that have access to College data.

1.4. Readers should note that the appendices of this policy and any referenced standards are enforceable as part of the policy and are subject to change.

1.5. Note: Throughout the policy the terms data and information are used interchangeably.

1.6. Note: This policy applies to mobile devices as applicable. For additional requirements pertaining to tablets and smartphones see Mobile Device Policy (**12.5**).

2.0 PURPOSE

2.1. Provide policy to secure Personally Identifiable Information (PII) of College employees, students, and others affiliated with the College, and to prevent the loss of information that is critical to the operation of the College.

2.2. Provide reasonable and appropriate procedures to assure the confidentiality, integrity, and availability of the College's information technology resources.

2.3. Prescribe mechanisms which help identify and prevent the compromise of information security and the misuse of College data, applications, networks, and computer systems.

2.4. Define mechanisms which protect the reputation of the College and allow the College to satisfy its legal and ethical responsibilities with regard to its networks' and computer systems' connectivity to networks outside the College.

2.5. Provide written guidelines and procedures to manage and control information considered to be PII whether in electronic, paper, or other forms.

2.6. Protect the integrity and validity of College data.

2.7. Assure the security and protection of PII in the College's custody, whether in electronic, paper, or other forms.

3.0 DEFINITIONS

3.1. *Centralized Computer Systems* - Computer hardware (including but not limited to servers, routers, switches, and access points) and software systems (including but not limited to Web hosts, customized databases, College databases, and faculty developed software for educational purposes) maintained by the IT Division and located in areas managed by IT personnel.

3.2. *Computing Equipment* - All hardware used to process, store, or transmit College data.

3.3. *Data* - Information contained in either College computer systems or in physical copy that is utilized for the purposes of conducting College business or learning.

3.4. *Decentralized Computer Systems* - Computer hardware (including but not limited to servers, routers, switches, and access points) and software systems (including but not limited to Web hosts, customized databases, College databases, and faculty developed software for educational purposes) maintained by any non - IT Division department.

3.5. *Information Technology Resource (IT Resource)* - A resource used for electronic storage, processing or transmitting of any data or information, as well as the data or information itself. This definition includes but is not limited to electronic mail, voice mail, local databases, externally accessed databases, CD-ROM, recorded magnetic media, photographs, digitized information, or microfilm. This also includes any wire, radio,

electromagnetic, photo optical, photo electronic or other facility used in transmitting electronic communications, and any computer facilities or related electronic equipment that electronically stores such communications.

3.6. *Kiosk* - Computers located in public spaces designed to offer limited functionality with specialized hardware or software.

3.7. *Lab* - A collection of computers that are either available for general use or are in a secured academic environment that are intended for specific use by students, faculty or staff.

3.8. *Mobile Device* - Any handheld or portable computing device including running and operating system optimized or designed for mobile computer, such as Android, Apple's iOS, or Windows Mobile. Any device running a full desktop version operating system is not included in this definition.

3.9. *Portable Equipment* - Laptops and other removable storage devices such as flash drives.

3.10. *Public Information* - Information that may be provided openly to the public.

3.11. *Security* - Measures taken to reduce the risk of (a) unauthorized access to IT resources via logical, physical, managerial, or social engineering means; and/or (b) damage to or loss of IT resources through any type of disaster, including cases where a violation of security or a disaster occurs despite preventative measures.

3.12. *Personally Identifiable Information: (PII)* Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on Snow College interests, the conduct of College programs or the privacy to which individuals are entitled. Examples of such data would include that data protected by the Government Records Access and Management Act (GRAMA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) or other laws governing the use of data or data that has been deemed by the College as requiring protective measures. Also included in this class of information are credit card and Social Security numbers. (For additional information on data classification types, reference policy 12.2 Data Classification and Handling.)

3.13. *Strong Password* - A password that is at least 8 characters long and is a combination of upper and lower case letters, numbers and special characters. Strong passwords do not include commonly used phrases, names, or other types of dictionary words.

3.14. *User* - All persons and/or organizations that have access to College data.

3.15. *Workstation* - Computers assigned to one or more College employees for conduction College business.

4.0 POLICY

Information security or protection of confidential personal and internal information departments and other College units must take measures to protect PII and internal information that is used, processed, transmitted, or stored on IT resources in accordance with this policy and any additional information security rules developed by data stewards and/or ISO.

4.1. *Information Confidentiality and Privacy.* All users are expected to respect the confidentiality and privacy of individuals whose records they access. Users are responsible for maintaining the confidentiality of data they access or use and the consequences of any breach of confidentiality.

4.2. *Handling Sensitive/Restricted Information.* The unauthorized addition, modification, deletion, or disclosure of PII included in College data files is expressly forbidden.

4.3. *Centralized/Decentralized Computing Systems.* All computing systems will be in compliance with this policy and College Security standards regardless of whether they are centralized or decentralized. Any decentralized computing systems that are unable to comply with the requirements of this policy may be required to relocate to the College Data Center at the discretion of the ISAC and ISO.

4.4. *Personally Identifiable Information Collection.* PII must only be collected for lawful and legitimate College purposes according to the requirements outlined in Utah System of Higher Education (USHE) Policy R345 – Information Technology Resource Security.

4.5. *Public Information.* Although there are no restrictions on disclosure of public information, the same precautions prescribed in this policy for protection of College data must be adhered to for the purpose of preventing unauthorized modification, deletion, etc. of public information.

4.6. *Access Control.* Access to College data and its resident computing system will be restricted to those users that have a legitimate business or educational need and appropriate approvals for access to such information. Users must ensure that PII is secured from unauthorized access and are responsible for safeguarding this information and related computing systems at all times through the use of strong passwords and as outlined in the Access Control Section of Appendix B.

4.7. *Remote Access.* Only authorized users will be permitted to remotely connect to College computer systems, networks and data repositories to conduct

College related business as required by the standard for secure remote access.

4.8. *Physical Security.* The physical security of computing resources will be accomplished utilizing current industry standards and appropriate technology and plans as defined by the ISO. Responsibility for centralized computing systems security will reside with the IT office. All other computing systems security will be the responsibility of the appropriate IT office specialist. See the Physical Security section of Appendix B for specific requirements.

4.9. *Data Security.* Users will ensure PII is secure and the integrity of records is safeguarded in storage and transmission. Users who handle PII are responsible for the proper handling of this data while under their control. Refer to the Data Security section of Appendix B for specific Data Security Requirements.

4.10. *Backup and Recovery.* Administrators of centralized computing systems will backup essential College data according to a documented disaster recovery plan consistent with industry standards and store such data at a secure commercial site. Decentralized computing systems will have available, at a minimum, a documented disaster recovery plan covering backup procedures, timelines, storage locations/procedures, and recovery.

4.11. *Security Incident Response and Handling.* All suspected or actual security breaches of College or departmental system(s) will be reported immediately to the organization's data security steward who will consult with the ISO to assess the level of threat and/or liability posed to the College or affected individuals and respond according to incident response guidelines maintained by the ISO. The College will report and/or publicize unauthorized information disclosures as required by law or specific industry requirements.

4.12. *Service Providers.* Service providers utilized to design, implement, and service technologies must provide contractual assurance that they will protect the College's PII it receives according to College or commercially reasonable standards. Such contracts must be reviewed by College Legal Counsel for appropriate terminology regarding use and protection of PII.

4.13. *Training and Awareness.* Each new College employee will be trained on the IT Technology Acceptable Use Policy and College Information Security Policy as they relate to individual job responsibilities. Such training will include information regarding controls and procedures to prevent employees from providing data to an unauthorized individual. All employees will be required to complete additional security training as prescribed by the ISO.

4.14. *Computer Labs.* Snow College provides robust computing lab resources for utilization in legitimate and lawful academic endeavors. Computing equipment in these labs will conform to all requirements of this policy with the addition of requirements stated in the Computing Lab Section of Appendix B.

4.15. *Software.* Only properly licensed software may be installed on College computer systems.

4.16. *Penalties and Enforcement.* Penalties and enforcement of this policy will be in accordance with College policies. Appropriate disciplinary and/or legal action will be taken when warranted in any area involving violations of this policy.

4.17. *Policy Review and Revision.* This policy and its associated appendices will be subject to periodic review and revision.

4.18. *Policy Clarification.* For clarification or further information on any items in this policy, the user is encouraged to contact the ISO, their data security steward or a member of the ISAC.

4.19. *Exceptions to Policy.* Any computing system that is unable to comply with this policy must file an exception. Exceptions to this policy must be approved by the ISO based on academic or business need and reviewed by the ISAC. The ISO will review exceptions annually for continued application and notify the exception holder of any concerns.

4.20. *Additional Policies.* Users should be aware that there are additional policies from other governing bodies that affect information security on campus and are outside of the College's Policy and Procedures Manual. Users should be familiar with the policies listed below and ensure their security practices are in adherence to these policies at all times.

4.20.1. Board of Regents (BOR) R345 - Information Technology Resource Security

5.0 SCOPE

5.1. This policy covers paper-based and electronic data defined to include, but not be limited to, all information maintained, processed, or distributed by the College computer systems that contain data defined by law or policy as PII. This policy also applies to all persons and organizations that have access to College data.

APPENDIX A: ROLES AND RESPONSIBILITIES

The persons responsible for implementing this policy and their respective duties and/or responsibilities with respect to this policy are described here.

College Deans/Managers/Supervisors - These individuals shall be responsible for oversight of their employees' authorized use and access to College data in their areas of supervision. They will:

- Ensure that the management and control of risks outlined in this policy are adhered to by employees in their unit.
- Ensure employees' access to College data is appropriate.
- Regularly review and document employee access to College data.
- Identify the necessary Data Security Steward and ensure they receive adequate training to perform this role.
- Provide employees with resources and methods to properly secure equipment where College data is processed, stored, or handled.
- Provide employees with approved resources and methods for external data storage where College data is processed, stored, or handled.

IT Specialist - These individuals are responsible for being the technical support within a business unit, college/school, or department.

Data Security Steward - These individuals are responsible for business processes within their areas of supervision will:

- Understand current information security policies, standards and guidelines and act as a point of contact for questions regarding information security and direct the user to the appropriate source (e.g., the ISO, policies, or standards).
- Operate as information security monitors in their divisions or colleges.
- Attend and participate annually in data security steward training provided by the ISO.
- Be the primary point of contact for suspected or actual data breaches and report the information to the ISO.
- Promote information security events/training and generate a culture of information security awareness.
- Recommend employees with access to PII data to the ISO for additional levels of training.
- Provide recommendations for revisions to this policy as appropriate.

Employees, including department chairs, faculty, staff, and student workers - These individuals:

- Shall not disclose PII College data to unauthorized individuals.
- Shall not modify or delete College data unless authorized by the Data Owner to do so.
- Shall maintain College data in a secure manner.
- Shall complete the employee/student confidentiality training.
- Shall be required to sign a College confidentiality/FERPA agreement before access is granted to PII College data.
- Shall complete specific confidentiality training if they have job related responsibilities that require access to PII College data.

Network Security Administrator - This individual, within the IT Division will:

- Implement adequate security measures for computing systems containing College data within their jurisdiction.
- Implement appropriate security strategies for both the transmission and the storage of College data.
- Notify appropriate units of possible security infringements.
- Report any security breach to the ISO.
- Disseminate technical guidelines related to security to the appropriate IT Specialists.

Information Security Advisory Council – A group of individuals appointed by the President to review and evaluate College security issues such as:

- Current practices and the associated risks to the institution.
- Actions needed to address those risks through appropriate policy and associated guidelines.
- Identify new processes that are needed.
- Implement new security standards as needed.
- Disseminate general guidelines related to security to the appropriate IT specialists.
- Function as the incident response team
- Responsible for immediate response to any breach of security.
- Responsible for determining and disseminating remedies and preventative measures that are developed as a result of responding to and resolving security breaches.
- Report findings and recommendations regarding the incident to data stewards and College administration.

Information Security Office – This office, within the Business and Finance Division will:

- Assist the campus in identifying internal and external risks to the security and confidentiality of information.
- Provide guidance for handling College data in the custody of the College.
- Provide guidance for the security of the equipment or data storage devices where the information is processed and/or maintained.
- Promote and encourage good security procedures and practices.
- Develop and maintain Information security policy, plans, procedures, strategies, and best practices.
- Assist institutional or third-party auditors in the analysis of College information assets and IT resources to further ensure policy compliance.
- Provide standards and guidelines consistent with College policies.
- Develop and provide information security training.

Internal Auditor – Internal auditor will:

- Evaluate the effectiveness of the current safeguards for controlling security risks.
- Provide recommendations for revisions to this policy as appropriate.
- Develop and perform random audits of departments and individuals as deemed necessary.

APPENDIX B - STANDARDS AND GUIDELINES

ACCESS CONTROL

- Automatic logins may only be enabled on kiosks and digital signage. These are limited access accounts specifically designed for this purpose.
- PII, electronic or paper, must not be left in an accessible location to prevent unauthorized viewing and must be secured when unattended.
- All users of computing systems that contain College data must have their own user name and use a strong password. The sharing of user names and passwords is not allowed.
- The password of empowered accounts, such as system administrators, must be changed every 120 days or require multi-factor authentication.
- Passwords used for College access must not be the same as passwords used for personal accounts (banks, personal email, and credit cards).
- Passwords must not be a user's Badger username, name or a word found in the dictionary.

- Passwords must not be placed in emails unless they have been encrypted.
- First-time passwords for new users must be set to a unique value for each user and changed after first use.
- Passwords must not be written down in a visible or accessible location.
- Periodic user access reviews should be conducted by the organization's supervisor and any unnecessary user access should be reported to IT Division and Human Resources and removed immediately.
- All workstations and lab computers must have a form of auto-lock feature enabled that requires a password to resume and set to activate at no more than an idle time of 20 minutes.
- Workstations visible to or accessible by anyone other than the authorized user must be manually locked when left unattended.

PHYSICAL SECURITY

- At a minimum, users shall comply with generally accepted College procedures to protect physical areas that contain College information.
- Individual organizations/departments within the College are responsible for physical security for personal computers and other local electronic information resources, including portable equipment, housed within their immediate work area or under their control.
- PII must only be used temporarily on portable equipment and then only for the duration of the necessary use and only if encrypted and physically secured.
- All College-owned computing equipment must be documented and managed in either a College-approved database or by property control.

DATA SECURITY

- All computing systems must install the College-approved management policy framework to manage antivirus and anti-spyware software as defined by the ISO in conjunction with the campus technology staff and leadership.
- PII data may only be stored on personal computers, servers or other computing equipment if the requirements outlined in USHE Policy R345, Information Technology Resource Security, are adhered to.
- All desktop systems and servers that connect to the network must be protected with a College-approved licensed anti-virus software product that is kept updated with the latest DAT files and anti-spyware software according to the vendor's recommendations.
- Headers of all incoming data, including electronic mail, must be scanned for viruses by the email server. Outgoing electronic mail must also be scanned for viruses.

- All servers must be approved and hardened with the IT Division before they will be allowed to transmit data through the Snow College firewall.
- Encryption technology will be utilized for local, portable, or central storage and transmission of PII.
- All transmission of PII via the Internet must be through a properly secured connection point to ensure the network is protected.
- All workstations and kiosks connected to the Internet will have a vendor supported version of the operating system installed with the option enabled to automatically download and install software updates or must utilize administrator managed patch management software.
- Software with the ability to serve information over the internet, must be disabled on all kiosks, workstations and lab computers.
- Peer-to-Peer (P2P) must be disabled on all kiosks, workstations, and lab computers.
- The file and printer sharing firewall exception must be disabled on all kiosks, workstations, and lab computers.

COMPUTING LABS

- All computing labs will utilize freezing or wiping software in such a way that minimizes the possibility of sensitive information from one user being accessible by any other user.

SNOW COLLEGE

Policy #12.5
Date Approved:
Date Amended: 1-27-2017
Responsible Office: Information Security

SUBJECT: MOBILE DEVICE POLICY

1.0 PURPOSE

Snow College is committed to and encourages an open and collaborative environment through the use of mobile devices to facilitate academic interaction among students, faculty and staff. There is an inherent risk in utilizing mobile devices for this purpose, however, due to the ease with which these items can become lost or stolen.

The purpose of this policy is to clearly state the college policy and user requirements necessary to mitigate this risk and to protect the college or Personally Identifiable Information (PII) stored on mobile devices.

2.0 POLICY

It is the responsibility of anyone who utilizes the Snow College internal network for the purpose of accessing or processing College PII using a mobile device to take appropriate measures at all times to safeguard that information.

All such individuals ("Users") will ensure they are taking every reasonable precaution against accidental or intentional data compromise by implementing the measures prescribed in Appendix A of this policy for their mobile devices.

3.0 DEFINITIONS

3.1. *Mobile Device.* Any handheld or portable computing device including running an operating system optimized or designed for mobile computing, such as Android, Apple's iOS, or Windows Mobile. Any device running a full desktop version operating system is not included in this definition.

3.2. *Personally Identifiable Information (PII).* Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on Snow College interests, the conduct of College programs or the privacy to which individuals are entitled. Examples of such data would include that data protected by the Government Records Access and Management Act (GRAMA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) or other laws governing the use of data or data that has been deemed by the College as requiring protective measures. Also included in this class of information are credit card and social security numbers

3.3. *Personal Identification Number (PIN).* This can be any combination of numbers (usually a minimum of four (4)) that is used to unlock a device.

3.4. *Encryption.* The use of software or hardware to make data unreadable unless the device is presented with the correct password or PIN. Most mobile devices include this feature but require the user to enable it.

3.5. *Remote Wipe.* The ability to erase all data on a device when the user and the device are physically separated. This is most often done through a service that the manufacturer provides via a website.

3.6. *Malicious Software.* Often called malware, this is software designed to disrupt computer operation, gather PII, or gain unauthorized access to computer systems.

3.7. *Anti-virus Software.* Software designed to detect and/or remove malicious software and viruses from a computer system.

3.8. *Data Security Steward.* Individuals within the different College organizations, appointed by the division dean who are points of contact for security violations or issues and act as a general reference within their work centers for information security topics.

3.9. *Strong Password.* A password that is at least eight (8) characters long and is a combination of upper and lower case letters, numbers and special characters. Strong passwords do not include phrases, names, or other types of dictionary words.

3.10. *Security Patch.* A fix to a program or application that eliminates a vulnerability exploited by malicious hackers. Most mobile devices will notify the user of updates to their installed applications that include the latest vulnerability fixes.

4.0 REFERENCES

Understanding and Identifying PII, Internal and Public Information

12.1 Information Technology Acceptable Use Policy

12.2 Data Classification and Handling Policy

12.4 Information Security Policy

Appendix A - Standards

- No mobile device shall be used to store PII unless the user complies with 12.4 Information Security Policy.
- All use of mobile devices, **College or personally owned**, which utilize College network resources, will be subject to the provisions of 12.1 Information Technology Acceptable Use Policy.
- All mobile devices will be kept up to date with the latest possible operating system, security patches, and application versions.
- All applications (apps) will be updated with the latest security patches.
- All devices will be configured with a PIN, pattern, or password-enabled lock screen configured to activate at no more than 5 minutes of inactivity.
- All devices with built in Encryption capability will have onboard Encryption enabled.
- All devices will have Remote Wipe enabled either through Mobile Sync, a third party app or the manufacturer's website.
- All devices that have been used to store, access and/or process PII will be wiped and overwritten to remove such data before they are transferred to someone else through sale or gifting.
- In the event that a device which has been used to store, access and/or process PII becomes lost, stolen or compromised, the owner must comply with the reporting requirements of 12.4, Information Security Policy. For a listing of the data security stewards by division, please refer to the data security stewards document maintained by the Information Security Office. Additionally, in case of loss, the user must immediately contact the IT service desk to request remote wiping through mobile sync if that service is utilized on the device. Otherwise, the user will request mobile wiping through the device's manufacturer.

SNOW COLLEGE

Policy #
Date Approved:
Date Amended:
Responsible Office: Controller's Office

SUBJECT: Cash Handling Policy

1.0 PURPOSE

To provide guidelines and procedures to ensure that all money paid to the College in the form of cash, checks or payment cards is properly receipted, accounted for, protected and deposited on a timely basis, and to ensure that the College complies with payment card industry data security standards.

2.0 DEFINITIONS

2.1 *Cardholder Data.* Data that contains the full card account number, expiration date and cardholder name.

2.2 *Card Validation or Security Code.* Three or four digit number printed on either the back or front of a credit card.

2.3 *Cash.* Cash consists of currency, coins, checks, money orders, and traveler's checks.

2.4 *Cash Change Fund.* A fund of money consisting of small currency bills and coins used to make change for larger currency bills tendered by a customer. The dollar value of a change fund always remains intact.

2.5 *Cash Receipting Center.* A department or office of the College, including individual Clubs, which is authorized to accept or take in cash receipts.

2.6 *Cash Receipts.* A term that represents all payment forms and includes cash, checks and payment cards.

2.7 *Cashier.* An individual whose job duties include the receiving, handling and processing of cash receipts.

2.8 *Deposit Transmittal Form.* This is a form created by the Controller's Office for each cash receipting center that is used to record all the revenue transactions into the College's accounting system. The transmittal form also documents the cash balancing and deposit preparation steps outlined in these procedures. The form shows the cash and check amounts that are to be deposited as well as payment card transactions that are electronically credited to the College's bank account.

2.9 *In-Person Cash Receipting.* This is a process when customers physically come to the cash receipting center to make purchases, payments, donations, etc.

2.10 *Payment Card.* A bank issued debit or credit card (i.e., Visa, MasterCard, American Express, and Discover) and the College Purchasing Card.

2.11 *Payment Card Industry Data Security Standards (PCI DSS).* These are standards established by the Payment Card Industry Security Standards Council. Any merchant that accepts payment cards is required to comply with these standards.

2.12 *PIN Block.* A block of data used to encapsulate a personal identification number (PIN) during processing.

2.13 *Separation of Duties.* The concept of having more than one person required to complete a task in order to lower the risk of fraud or error.

3.0 POLICY

College departments, offices or clubs shall receive written authorization from the Controller's office prior to handling cash receipts. This will ensure that all employees and students responsible for handling cash receipts are properly trained and controls are in place before accepting cash receipts. In addition, wherever payment cards are accepted as payment, the cashier will comply with the College's Payment Card Handling Policy.

4.0 PROCEDURES

4.1 Establishment of Responsibility and Internal Controls:

Because of the sensitive nature of cash receipts and cardholder data, it is important that responsibilities and procedures are clearly defined and followed by all employees involved with cash receipting. Defining responsibilities and procedures helps protect employees who handle or have access to cash receipts as well as the College from theft of money or cardholder data. Staff, faculty, volunteers, consultants, and students are responsible for compliance with these procedures. The establishment of strong internal controls and these procedures for cash receipt collections and payment card acceptance is necessary to ensure that all funds received are properly receipted, accounted for, safeguarded and deposited on a timely basis. Internal controls help prevent mishandling or loss of funds and the theft of personal payment card information.

4.2 Authorizing and Establishing a Cash Receipting Center:

4.2.1 Pre-authorization from the Controller's Office is required before cash receipts can be collected. Departments that wish to be a cash receipting center must submit a written request to the Controller's Office prior to accepting money that includes:

- Reason(s) why collecting cash receipts is needed.
- A list of individuals or positions that will be involved with the cash receipting process.
- Whether there is a need for a cash change fund, and the desired dollar amount thereof.
- Whether there is a need or expectation to accept credit and debit cards. Only the Controller's Office is authorized to establish new credit card merchant accounts and the department must be willing to accept costs associated with accepting payment cards.

4.2.2 After a request is received and approved, the Controller's Office will assist the department in establishing internal controls and procedures to help ensure money is accounted for, safeguarded and deposited at the Cashier's Office within three business days.

4.3 Operating Procedures for Cash Receipting Centers:

A list of required procedures to be implemented by each cash receipting center is as follows:

4.3.1 Every cash receipt transaction must be receipted and recorded through an approved cash register system or use of approved pre-numbered manual receipts. In each case, a receipt must be produced and presented to the customer at the conclusion of the transaction. Approved pre-numbered receipt booklets are available at the Cashier's Office.

4.3.2 Special attention should be taken to validate all "void, refund, cleared, or no-sale" transactions. A second person, such as another cashier or supervisor, should approve the transaction at the time it occurs by signing the void slip or receipt.

4.3.3 When pre-numbered manual receipts are issued, the unused inventory of receipts must be secured at all times. Copies of the used receipts (including those which are voided) and the unused receipts must be accounted for at all times and are subject to audit by the Controller's Office or the Office of Internal Audit.

4.3.4 Separation of employee duties, as established in conjunction with the Controller's Office, must be maintained at all times within the cash receipting operation.

4.3.5 As part of the deposit preparation process, all funds received must be reconciled to the cash register summary totals, such as the "Z" tapes, or to the pre-numbered receipts on a daily basis. Cash, checks and payment cards must be accounted for and reconciled separately. All void, refund, cleared, or no sale transactions should be highlighted and accounted for with each deposit. For ease in completing and documenting this reconciling process, a deposit transmittal form (see Attachment A) should be utilized for each deposit (also refer to sections 4.6 "Balancing of Cash Receipts" and 4.7 "Preparation of Deposits").

4.3.6 For each deposit, an independent person, one who does not have access to the cash receipts, must reconcile the bank or cashier deposit amount to the original cash register ("Z" tape) or other receipt summaries to help ensure that all funds that should have been received are actually deposited. Any void, refund, cleared or no sale transactions noted in the deposit backup should be reviewed for reasonableness. The person performing this independent reconciliation must sign on the deposit transmittal form to indicate this step has been completed.

4.3.7 All checks, cash and credit card receipts must be physically protected during the day by using a cash register or locking drawer; and if kept overnight, in a safe or other approved secure place until the money is deposited. Cash should only be kept in cash registers or locking drawer during hours of operation.

4.3.8 Credit Card machines (also known as "POS Device") must be physically protected in an approved secure place during the non-operating hours of the cash receipting center.

4.3.9 Cash registers or other locking drawers should be locked when not attended, even if the cashier only leaves the station for a brief period of time.

4.3.10 Money is not to be counted in public view. A secure area for counting and preparing the deposit must be provided and restricted to authorized personnel. Two people must be present while cash is counted.

4.3.11 Checks should be made payable to "Snow College" and must be endorsed promptly with a restrictive endorsement stamp payable to Snow College.

4.3.12 Checks or debit card transactions are not to be written or entered for more than the amount of purchase in order for the customer to get cash back.

4.3.13 Cash receipting centers are not allowed to cash personal checks from cash receipts.

4.3.14 All cash receipts should be deposited at the Cashier's Office window within 24 hours of receipt, and no later than the next business day. A College cashier window receipt shall be considered the same as a bank deposit receipt for the purpose of agreeing the independent reconciliation of the amount deposited back to the original supporting receipt documentation.

4.3.15 Under no circumstances may purchases be made directly from cash receipts (Example: taking cash from earnings in locking drawer to purchase office supplies or other items). Purchases can be made with a Snow College Purchasing Card or with an employee's personal funds which can then be submitted to the Accounts Payable office for reimbursement.

4.3.16 When an employee who has a key or safe combination to where money is held terminates employment, the key must be collected and the safe combination changed.

4.3.17 Any employee designated to be a cashier should receive training provided by the Controller's Office before working as a cashier.

4.3.18 Passing of a background check will be required for all new employees (whether a part time or full time employee) for a "full time" cashier position. A full time cashier position is one where the employee's primary duty is cashiering. Employment background checks are not required, but recommended for new employees where they may perform cashiering duties on a sporadic or occasional basis.

4.4 In-Person Cash Receipting Procedures:

4.4.1 A receipt must be created and presented to the customer for each payment received at any cash receipting center. At a minimum, manual pre-numbered receipts must include the date, method of payment (cash, check or credit card), and the identification of the department and the person issuing the receipt. If the receipt is not manually written, but rather produced from a cash register, the receipt should have similar information with the exception of method of payment.

4.4.2 Only one cashier is allowed access to a cash register or cash drawer during a single shift. The cash drawer should be closed out at the end of every shift so that only one person is responsible for the transactions and related cash receipts.

4.4.3 All checks received in person must have additional identification written on the check such as the student ID number, or driver's license number if not a student.

4.5 Cash Receipts Received Via Mail:

4.5.1 The mail must be opened with two people present and all checks should be immediately endorsed with a restrictive endorsement stamp and entered on a check log that is signed by both parties. This process is in place to establish receipt and fiscal tracking accountability/responsibility. The log should subsequently show the disposition of the checks, whether transferred to another person, department, or deposited at the Cashier's Office or bank. (See Attachment B)

4.5.2 Cash receipts received in the mail should be identified and officially receipted within one business day and deposited promptly according to section 4.3.14 or 4.7.1 of this policy.

4.5.3 Unidentified checks must be immediately forwarded to the Controller's Office for research and deposit.

4.6 Balancing of Cash Receipts:

4.6.1 At the end of each day and cashier shift, the cashier must close the batch or session and balance the money collected to the cash register or manual receipts. This is done by physically counting and comparing the total of the cash, checks and credit cards on hand (net of the cash change fund amount) to the cash register summary or to the pre-numbered receipts used during the session. Any dollar difference must be accounted for separately as an "overage" or "shortage" on the deposit transmittal or recap and must be investigated, documented and resolved to the extent possible. Documentation must include cashier and reviewer signatures.

4.6.2 All voided, refund, cleared or no-sale transactions should be approved by another person evidenced by the cashier's signature and the other person's signature. These transactions, in addition to overages and shortages, should be accounted for on the deposit transmittal form to be reviewed by a supervisor for validity, reasonableness and appropriateness. If a supervisor is unavailable, another employee may review the deposit transmittal form.

4.7 Preparation of Deposits:

4.7.1 Deposits made to the bank (Cashier's Office Only):

- Bank deposit slip booklets must be ordered and obtained from the Controller's Office.
- A calculator tape of the checks should be included with the checks bundled together.
- Cash and checks must be recorded on the deposit slip in the appropriate spaces.
- Once a deposit is final, the completed bank copy of the deposit slip, cash and checks must be put in sealable or locked deposit bags to prevent tampering.
- The Cashier's office shall make deposits to the bank within 24 hours, but no longer than every three days per State Law (Title 51, Chapter 4, Section 1).

- Where possible, two employees are required to transport the deposit to the bank together. Employees outside of the Cashier's Office are not to personally transport deposit bags to the bank unless approved to do so in writing by the Controller's Office or Vice President of Finance and Administration. If two employees are not available to take the deposit to the bank, then one employee shall prepare the deposit and a separate employee shall deposit the funds at the bank. The deposit slip from the bank shall be agreed to the Snow College deposit slip. Any differences shall be reported to the Controller's office.
- A daily cash report must be completed daily (see Attachment C). These reports shall be submitted to the Controller's Office at the end of each week. The daily cash report must show the cash and check amounts that were deposited and separately show the payment card transactions that were electronically credited to the College's bank account. Accordingly, a copy of the payment card batch summary shall be attached to the report.
- The returned bank deposit receipt should be filed with a copy of the daily cash report and cash receipts backup for subsequent audit purposes.

4.7.2 Deposits made at the Cashier's Office window:

- College departments, offices and clubs deposit money directly at the College cashier window. The cash receipts collected must be properly accounted for and entered into the College's accounting system by the Cashier's Office.
- The department's deposit transmittal form takes the place of a bank deposit slip when money is deposited at a cashier's window.
- A calculator tape of the checks should be included with the checks bundled together.
- Cash and checks must be recorded on the deposit transmittal form in the appropriate spaces.
- Once a deposit is final, the completed deposit transmittal form, cash, checks and payment card batch summary information must be put in a sealable or locked deposit bag to prevent tampering.
- When transporting deposit bags to the cashier's window, employees should exercise care to make sure that the bags are inconspicuous during transit. It is recommended, where possible, that two employees or students transport the deposit together or a Campus Security escort may be requested. A Campus Security escort is required if the cash deposit exceeds $8,000. If two employees or students are not available to take the deposit to the Cashier's office, then one person should prepare the deposit and a separate person should deposit the funds at the Cashier's Office. The deposit slip from the Cashier's Office should be agreed to the deposit transmittal form. Any differences should be reported to the Controller's office.

- A deposit transmittal form must be completed for every deposit taken to the cashier's window to document the deposit amount and to record all the revenue transactions into the College's accounting system. The deposit transmittal form must show the cash and checks amount that was deposited and separately show the payment card transactions that were electronically credited to the College's bank account. Accordingly, the payment card batch summary should be attached to the deposit transmittal form. In addition, for accounting purposes, the deposit transmittal form should have a line for each type of revenue received that contains a description of the type of transaction, the dollar amount, and the appropriate index and account numbers.
- The official cashier's receipt should be filed with a copy of the deposit transmittal form and cash receipts backup for subsequent audit purposes.

4.8 Independent Reconciliation of Cash Collected and Deposited:

For each cash receipting center, an independent person (one who does not have access to the cash receipts) must compare the total receipts to the deposit amount to help ensure that all funds that should have been received are actually deposited at the cashier's window. The independent person's duties include:

4.8.1 Reviewing the cash register transactions summaries, such as the "Z" tape, or manual pre-numbered receipts and comparing the total sales amounts that should have been collected to the deposit amount recorded on the copy of the deposit transmittal form.

4.8.2 Comparing the total from the deposit transmittal form to the deposit per the cashier window receipt.

4.8.3 Signing off on the deposit transmittal form copy or otherwise documenting that the above tasks were accomplished without exception. Any noted differences must be immediately reported to the Controller's Office.

4.9 Procedures When Using Pre-Numbered Manual Receipts:

In situations, such as certain special events, where mechanical cash registers are not available or practical, a pre-numbered receipt system must be used to document each sales transaction. Pre-numbered paper receipts must be obtained from the Cashier's Office. The Cashier's Office will maintain a log that records the number(s) of the blank, pre-numbered receipts issued, the date issued and the name of the person receiving the receipts. The department receiving the blank, pre-numbered receipts is responsible and accountable to the Cashier's Office for the proper handling of all the receipts (used and not used receipts). Therefore, the department must take steps to safeguard and protect the blank receipts from theft. As receipts are issued to customers for payment received, a receipt copy must be retained by the department, office or club for end-of-day balancing, deposit preparation and subsequent independent audit purposes.

4.10 Special Event Cash Receipting:

There may be certain temporary special events where the use of cash registers or pre-numbered receipts is not practical. For such an event, the organizing department must work with the Controller's Office to establish appropriate cash receipting methods that incorporate the principles covered in these procedures.

4.11 Cash Change Fund Procedures:

The dollar amount of a granted cash change fund will be determined jointly by the department, office or club, Cashier's Office, and the Controller's Office. The following guidelines pertain to cash change funds:

4.11.1 The exact amount of the cash change fund must always remain in place. It cannot be used to "cover" any cash shortages or overages. Therefore, at the end of each day or cashier session, the exact amount of the cash change fund must be counted and set aside before other cash receipts are counted and balanced for deposit purposes.

4.11.2 Departments, offices or clubs may exchange large currency bills for smaller bills and coins at any College cashier window.

4.11.3 Change funds are subject to unannounced audits by representatives of the Controller's Office or Office of Internal Audit.

4.11.4 Only one cashier is allowed access to a cash change fund during a single shift. The cash change fund should be closed out at the end of every shift so that only one person is responsible for the transactions and related cash receipts.

4.12 Petty Cash Procedures:

Departments, offices or clubs are not permitted to establish a petty cash fund.

4.13 Payment Card Data Security Procedures

For payment card handling procedures please refer to the College's Payment Card Handling Policy.

4.14 Cash Receipts for Donations and Sponsorships

4.14.1 Cash receipts for donations, gifts and sponsorships must comply with this policy. For further guidance on the handling of Donations and Sponsorship please refer to Section 17.0 of the Snow College Policies and Procedures Manual, *Advancement Office Policies and Procedures.*

4.15 Cash Payments

4.15.1 Currency and Coin Payments

4.15.1.1 Generally, cash payments are prohibited. Requests for exceptions must be submitted in writing to the Controller's office who will seek approval of the Vice President of Finance and Administration. Determinations whether to grant exceptions will be based upon available resources, risks and other circumstances surrounding the request.

4.15.1.2 If cash payment is approved, certain documentation will be required to be returned to the Controller's office within one business day of when the cash payment occurs. Documentation required will be determined on a case by case basis. In addition, if cash payment is greater than $2,000, a Campus Security escort will be required.

4.15.2 Check, Cashier's check or Bank Wire Payments

4.15.2.1 Please reference the Accounts Payable Procedures. See https://www.snow.edu/offices/controller/downloads/AP%20QandA.pdf

4.16 Exceptions to Above Procedures:

Requests for exceptions to these procedures must be submitted in writing to the Controller's Office for review and approval. Determinations whether to grant exceptions will be based upon available resources, risks and other circumstances surrounding the requesting cash receipting center.

5.0 REFERENCES

5.1. Utah Code, Title 51, Chapter 4, "Deposit of Funds"

5.2. Payment Card Industry Security Council – Current Data Security Standards: www.pcisecuritystandards.org

Attachment A

Deposit Transmittal Form

SNOW COLLEGE

Cashier's Office
150 College Avenue
Ephraim, Ut 84627
435.283.7000
www.snow.edu

Date: _____ Cash Box No. _____

Activity: _____

Account number for receipt/deposit: _____

Cash Change Fund: _____ Date of Activity: _____

Money Checked out by: _____

Beginning Receipt No. _____ Ending Receipt No. _____

CASH SUMMARY

COIN		CURRENCY	
$ 1.00	$	Cr Card	$
0.50	$	Checks	$
0.25	$	$100/$50	$
0.10	$	$20	$
0.05	$	$10	$
0.01	$	$5	$
		$1	$
TOTAL	$	**TOTAL**	$

Total Coin and Currency $ _____

Minus Cash Change Fund $ _____

TOTAL PROCEEDS $ _____

Less Total per Receipts $ _____

Overage/(Shortage) $ _____

Explanation of overage/Shortage: _____

Void/Refunded Receipt #	Receipt $	Reason	Initial #1	Initial #2
Total:	$ -			

1st Money Count completed by: _____

2nd Money Count completed by: _____

Cashier's Office Signature: _____

I have verified that the deposit per the Snow College Cashier's Office receipt agrees to the the "Total Proceeds" line on this form and will retain the receipt with a copy of this deposit transmittal form.

_____
(Signature)

The deposit per the Snow College Cashier's Office receipt does not agrees to the the "Total Proceeds" line on this form. I have contacted the Controller's office and will retain documentation of the resolution.

_____
(Signature)

Attachment B

SNOW COLLEGE

Check Log

Department:_____ **Date:**_____

Check No.	Check Date:	Date Received	Check Amount:	Payee:	Purpose:	Deposited into account:	Place of Deposit	Date of Deposit
EXAMPLES:								
1234	1/1/2017	1/5/2017	$ 10,000.00	Jane Doe	Science Building Campaign	R22905	Cashier's Office	1/6/2017
2345	1/10/2018	1/12/2017	$ 500.00	John Doe	Tuition Payment	Student #00123456	Zions Bank	1/12/2017
			$					
			$					
			$					
			$					
			$					
			$					
			$					
			$					
			$					
			$					
			$					
			$					
			$					
			$					
			$					
			$					
Total			$ 10,500.00					

The total number and dollar value of checks in this log is accurate and complete:

_____ (signature)

_____ (signature)

_____ (date)

Attachment C

Snow College - Cashier's Office
Daily Cash Report

Date:
Prepared By:
Session #:

Notes

CASH

Deposit to Bank		Calculation from Cash Report	
100.00	-		
50.00	-		
20.00	-		
10.00	-	Beginning	-
5.00		Banner Total	-
1.00	-	Checks	-
0.25	-	CC's	-
0.10	-	Noncash	-
0.05	-	Over/(Short)	-
0.01	-	Ending	-
Cash Deposit Total:	-	**Cash Deposit:**	$ -
Initial:		Over/(Short)	-

Checks

$ -

Credit Cards

Cashier's Office		
AC/Athletics	$	-
Registrar's Office	$	-
Eccles	$	-
Snow College/Foundation	$	-
Cafeteria	$	-
TOTAL CCs:	$	-

Non-Cash Transactions:

Charges	$	-
Negative Payment (Payment)	$	-
Total	$	-

Report Total

$ -

Total From Banner Report

Total Over/(Short)

$ -

Nelnet:

Nelnet_user	$	-
Nelnet	$	-
Admission Fees	$	-
www User	$	-
Nelnet Total	$	-

SNOW COLLEGE

Policy #
Date Approved:
Date Amended:
Responsible Office:

SUBJECT: SCHEDULING CAMPUS FACILITIES

1.0 PURPOSE

1.1. The Utah State Board of Regents has directed each institution to develop policies that provide convenient and appropriate means for approving and scheduling the use of campus facilities. Snow College (Snow) strives to serve its campus community and the community at large by offering its facilities for use when possible. This policy governs how requests for the use of Snow facilities are approved, what requirements those using Snow facilities must meet, and what types of fees are charged for college and non-college groups.

2.0 DEFINITIONS

2.1. *Co-sponsored events:* Events that are the result of a formalized professional relationship between college and non-college entities. These events include, but are not limited to, conferences, programs, workshops, activities, or seminars held at college facilities and properties.

2.2. *Fronting:* When a college or non-college individual or organization uses college space/facilities and services under the false representation to the scheduling office that the activity is a co-sponsored event.

2.3. *Non-profit entity:* An organization with IRS 501C3 or 17061A status.

2.4. *Non-college entity:* Any non-Snow group that is not covered by the State of Utah Risk Management insurance and receives no operational funding from Snow.

2.5. *College group:* Any group funded by Snow and covered by the State of Utah Risk Management insurance.

~~2.5.~~2.6. *Facilities:* College controlled property including, but not limited to, college buildings, grounds, practice fields, and other holdings.

3.0 POLICY

3.1. Use of campus facilities, whether by non-college or college group, shall not interfere with instructional activities or any other part of the institution's mission, unless receiving prior approval from the Vice President of Academic Affairs. Co-sponsored events shall follow the same requirements as college groups.

3.2. Fronting, as defined in section 2.2, is prohibited.

3.3. The scheduling office is designated by the President for scheduling college facilities. The scheduling office shall inform both college and non-college groups of Snow policies and procedures to ensure all requirements are met prior to use of the facilities.

3.4. All events must be scheduled through the scheduling office. Requests to use college facilities may be reviewed for health and safety concerns and for

Formatted: Underline, Font color: Red
Formatted: Underline
Formatted: Underline, Font color: Red
Formatted: Underline
Formatted: Underline, Font color: Red
Formatted: Underline
Formatted: Underline, Font color: Red
Formatted: Underline
Formatted: Underline, Font color: Red
Formatted: Underline

compliance with college policy and with state and federal law. Appeals to the decision of the scheduling office may be made to the Vice President for Finance and Administration.

3.5. Each co-sponsored event must be supported in full or part by a college ~~department, Student Life, or college-chartered club~~ group. College groups must assume responsibility for any costs that may be associated with the event. The college group must have a major role in the planning and hosting of the event and provide services and resources for the event. A representative of the college group must execute an appropriate college agreement prior to the event.

Formatted: Font color: Red, Strikethrough

3.6. The club must be ~~heavily~~ involved with all aspects of the planning and publicity and is required to participate in the event. Only the authorized club officer or faculty sponsor may submit scheduling requests.

Formatted: Font color: Red, Strikethrough

3.7. The non-college group must also be involved in the planning and implementation of the co-sponsored event.

4.0 PROCEDURES

4.1. The President has designated a scheduling office with the responsibility for scheduling college facilities.

4.2. Scheduling, Fees and Snow Food Services

4.2.1. All non-college or college department co-sponsored events must be accompanied by a rental/use agreement prepared by the scheduling office. Refer to the scheduling office's website for fees, cancellation policy and related information.

4.2.2. For all scheduled events in college facilities, any and all food must be scheduled through Snow Food Services. On-campus groups may provide their own food with written approval from Snow Food Services. Snow Food Services has first right of refusal for providing food and beverage service for all events scheduled on Snow's Ephraim campus (Richfield campus excluded). If Snow Food Services cannot accommodate the request outside sources may be considered.

4.3. Fronting

4.3.1. When it is determined that college and/or non-college groups have been fronting, their event will be canceled and they will be charged the full rental fee for the event.

4.3.2. Non-college groups that have engaged in fronting shall be forbidden from scheduling any events in the future on college property.

4.3.3. College groups that have engaged in fronting may be charged a rental fee for the current event and any future events; college employees that have engaged in fronting may face discipline.

4.4. Use of College Facilities by College Groups

4.4.1. College department or state entities may be required to pay expenses including, but not limited to staffing, custodial, sound and lighting, piano tuning and moving, security, etc. An estimate of these expenses will be provided before entering the required use agreement. An estimate is not binding; other costs that may arise will be billed.

4.4.2. Scheduling requests for college-chartered clubs must be made by the club officer or club advisor.

4.5. Use of College Facilities by Non-College Groups

4.5.1. For non-college groups requesting space for the sole purpose of hosting a meal fully catered by Snow Food Services, no insurance is required.

4.5.2. All non-college groups and department co-sponsored groups are ~~required~~ subject to pay a rental fee and expenses. Formatted: Font color: Red, Strikethrough

4.5.3. Non-profit organizations will be charged half-price rental for all college facilities. Documentation is required as proof of IRS501C3 and 170B1A status.

4.5.4. ~~Only the Campus Scheduling is authorized to schedule department labs, fields, etc., for non-credit events and/or to non-college entities. College groups or non-~~ Non-college groups that wish to schedule ~~these~~ college facilities for non-credit events must do so through ~~Campus Scheduling~~ the Scheduling Office when a financial transaction is involved. Formatted: Font color: Red, Strikethrough Formatted: Font color: Red, Strikethrough Formatted: Font color: Text 2, Strikethrough

4.6. Requests to Film or to Perform Photo-shoots on Snow Campus

4.6.1. Requests to film or perform photo-shoots on campus shall not interfere with any previously scheduled events.

4.6.2. The scheduling of all non-college groups requests for filming (which also includes the filming of conference and workshop sections) or performing photo-shoots requires the following approvals.

4.6.2.1. The scheduling office must approve the filming or photo-shoot date and time.

4.6.2.2. The scheduling office will send the film script or photo-shoot description to the Public Relations Director and Assistant to the President for review and approval. This

approval must be obtained at least five (5) business days prior to the requested date of filming or shooting.

4.6.3. The scheduling of filming for academic classes must have the approval of the Institutional Research Director at least five (5) business days prior to the requested date of filming. Class instructors shall review and approve the topics covered by student filming. Instructors are required to submit scheduling requests on behalf of their students.

Snow College Concurrent Enrollment Policies

These policies are specific to Snow College and are in addition to the Board of Regents Policy R165 (https://higheredutah.org/policies/policyr165/) and the Utah Concurrent Enrollment Handbook (http://www.schools.utah.gov/CURR/earlycollege/Concurrent-Enrollment/UtahHandbook.aspx).

1. **Eligibility**
    a. Only seniors can take ENGL 1010.
    b. Only seniors completing a General Education Certificate or Associate's Degree can take ENGL 2010 and/or PE 1096.
    c. To enroll in a literature class, students must have taken English 1010 or must be taking it concurrently.
        i. Juniors (and seniors without 1010) may petition to enroll in a literature class by:
            1. having at least a 20 on the English ACT,
            2. submitting a short recommendation from a high school counselor, and
            3. completing a placement exam.
        ii. Note: petitions may take up to a week to consider.
    d. Only juniors or seniors will be enrolled in Hybrid classes. High school counselors must submit an online Hybrid Request Form to enroll a student in a Hybrid class. The Hybrid Request Form will be viewed as the student's Add Form, but does not guarantee them a spot in the class. The counselor and student must have a plan on when and where the student will access recorded lectures on a regular basis. Watching Hybrid recorded lectures must occupy a class period on the student's high school schedule; students cannot plan to watch recorded lectures at a location other than the high school or outside the high school's normal hours.
    e. Counselors must submit an online Sophomore by Exception request form for each sophomore or freshman wishing to enroll in any courses. Sophomores and freshman must have a high school GPA of 3.5 or higher.
    f. Sophomores and freshman will not be allowed to enroll in the following courses:
        i. CHEM 1110/1115
        ii. COMM 1020 (unless there are seats available not filled by juniors or seniors)
        iii. ENGL 1010
        iv. ENGL 2010
        v. HFST 1500
        vi. Literature courses
        vii. PE 1096
        viii. PSY 1010
        ix. SOC 1010
    g. If a student earns an "F" in a Snow College concurrent enrollment course, that student will not be allowed to take any additional concurrent courses from Snow College.

2. **Enrollment**
    a. Each semester students at rural high schools shall be allowed to enroll in Snow College IVC classes two weeks before general registration is opened to students at non-rural high schools. Rural high schools shall be defined as those in the following counties: Beaver, Carbon, Daggett, Duchesne, Emery, Garfield, Grand, Iron, Juab, Kane, Millard, Morgan, Piute, Rich, San Juan, Sanpete, Sevier, Summit, Tooele, Uintah, Wasatch, Washington and Wayne.
    b. Students are encouraged to take courses as Face-to-Face (F2F) from a qualified teacher at their high school whenever possible. If a F2F course does not fit the student's need, then an IVC course is the next best option. Students should consider taking a course as a Hybrid only when another format (F2F or IVC) is not possible.
    c. Online enrollment will be shut down each semester after the fifth day of class. After that enrollments can only be done with a paper Add Form and the instructor's approval.
    d. Class rolls for F2F classes will be frozen on October 1 for fall semester and February 1 for spring semester. After those dates, students will not be added to F2F class rolls.
3. **Miscellaneous**
    a. IVC students must be in their seats at the beginning and ending of each class. Any overlap with other courses not on Snow's IVC schedule must not cut into the time the student is in the IVC class.
    b. High school facilitators are an extension of the professor and are expected to help maintain a healthy classroom environment. Snow College has online training which high school facilitators must complete each year.
    c. Students taking nine or more concurrent enrollment credit hours in a semester, or who have earned a total of 20 or more concurrent enrollment credits, must meet with a Snow College Academic Advisor to discuss their academic goals.
    d. Students, or their high schools, will be responsible for providing required textbooks for courses.

MONTANA STATE UNIVERSITY

Free Speech Policy

Subject:	Governance and Organization
Policy:	Freedom of Expression Policy
Effective Date:	September 7, 2011
Revised Date:	February 2, 2012
Review Date:	September, 2014
Responsible Party:	Office of Legal Counsel

Introduction and Purpose

MSU recognizes that the freedom of expression is integral to the purpose and process of the University, whose primary goal is education. Therefore, no University policy or rule will infringe upon this constitutional right.

Policy

MSU supports and encourages diverse points of view, though they may sometimes seem distasteful or offensive, as this is the nature of the University's educational responsibility and is safeguarded by the freedom of expression. The acceptance of diversity is a fundamental tenant of the Land Grant University system, and is instrumental to the creation of new discourses and the weighing of different views.
MSU recognizes the First Amendment rights to expression. These rights include individual and group activities including but not limited to:

- Assembling,
- Demonstrating,
- Signing,
- Pamphleting,
- Structuring, and
- Political campaigning.

Procedures

The right to freedom of speech includes exercising it responsibly, including abiding by the following:

MONTANA STATE UNIVERSITY

Free Speech Policy

Subject:	Governance and Organization
Policy:	Freedom of Expression Policy
Effective Date:	September 7, 2011
Revised Date:	February 2, 2012
Review Date:	September, 2014
Responsible Party:	Office of Legal Counsel

Introduction and Purpose

MSU recognizes that the freedom of expression is integral to the purpose and process of the University, whose primary goal is education. Therefore, no University policy or rule will infringe upon this constitutional right.

Policy

MSU supports and encourages diverse points of view, though they may sometimes seem distasteful or offensive, as this is the nature of the University's educational responsibility and is safeguarded by the freedom of expression. The acceptance of diversity is a fundamental tenant of the Land Grant University system, and is instrumental to the creation of new discourses and the weighing of different views.
MSU recognizes the First Amendment rights to expression. These rights include individual and group activities including but not limited to:

- Assembling,
- Demonstrating,
- Signing,
- Pamphleting,
- Structuring, and
- Political campaigning.

Procedures

The right to freedom of speech includes exercising it responsibly, including abiding by the following: