

Prepared by: Data Access Policy Project Team
Approved by: CITC, May 2007

Keene State College
Campus Data Access Policy

Table of Contents

<u>Section</u>	<u>Page</u>
I. Why we have this policy.....	4
A. Scope of Policy	4
B. What is covered.....	5
C. What is not covered	6
D. Guiding Principles	6
II. Data Classification	6
IV. Roles and Responsibilities	7
A. Administrative Officials.....	7
B. Campus IT Security Manager	7
C. Data Proprietor.....	7
D. Data Custodian (includes Department Application Techs)	8
E. Campus Information Technology Group	9
F. Data Integrator	10
G. Data User	10
V. Procedures.....	11
A. Best Practices	11
1. Data Management	11
2. Restricted Data.....	12
3. Administrative Data of Record and Unofficial Data	12
4. Computer Security	13
5. Systems Development (department and central databases and systems).....	14
6. Vendor Relationships.....	14
B. Special Cases	14
1. Survey Data.....	14
2. Marketing Data	15
3. Outsourced Data.....	15
4. Office and or Function Specific Data Bases/ Systems.....	16
VI. Policy Implementation	17
A. Training.....	17
B. Enforcement.....	17
1. Who and how	17
2. Violation of Policy and Misuse of Data.....	17
3. Arbitration of Disputes	18
VII. Glossary	19
VIII. Related Documents	22
A. Federal Regulations	22
B. State Regulations	22
C. USNH Policies	22
D. KSC Policies	22
VIII. Attachments	23
A. Attachment #1 – Suggested Clauses for Service Provider Agreements	24

Prepared by: Data Access Policy Project Team

Approved by: CITC, May 2007

Policy Summary

This document sets forth the college's policies with regard to the proper management, access, use, and reporting of Keene State College (KSC) administrative data. It includes data stewardship roles and responsibilities, standard definition of terms and procedures for carrying out these responsibilities. This policy is intended to foster clear accountability, increase effectiveness of data administration, and minimize legal exposure and liability associated with improper use of campus data.

The policy applies only to data owned by the College. Campus Data includes all data prepared, supplied, used or retained by college employees, within the scope of their employment, or by agencies or affiliates of the school, under a contractual agreement, except for data specifically excluded from school ownership by law, policy, or special overriding ownership provisions. This includes data created through all college operations (primary databases), secondary or tertiary databases, and information used for both internal and external purposes.

With the implementation of Datatel and increased access to data campus-wide, a policy is needed to address the issues of information stewardship, access, and responsible use and reporting of data in order to reduce the risk of data compromise and inconsistency, and violation of confidentiality.

Campus administrative data can be ...

- contained in any form, including but not limited to documents, spreadsheets, databases, email, and web sites.
- represented in any form including but not limited to letters, numbers, words, pictures, sounds, symbols, or any combination thereof.
- communicated in any form including but not limited to handwriting, typewriting, printing, photocopying, photographing, and web publishing.
- recorded upon any form including but not limited to papers, maps, films, prints, microfiche, discs, drives, and other devices.

The policy defines the classification of data by levels of sensitivity and criticality and by status of use, so preparers, suppliers, and users of campus data can understand the types of data within their custody and the business rules that apply to the data. Data generally falls into the following categories: restricted or unrestricted; essential, required, or deferrable; data of record or unofficial data.

The policy identifies and interprets applicable federal and state laws, as well as Keene State College policies both formal and informal. In the event that this policy conflicts with existing federal or state law or college policy the federal or state law or college policy will take precedence.

I. Why we have this policy

The implementation of a central integrated Student Information System (SIS) and Alumni/Advancement system from Datatel has resulted in increased access to data campus-wide and the increased distribution of the data to secondary and possibly tertiary databases and systems. A policy is needed to address the issues of information stewardship, access, responsible use and reporting of data, and disposal of data in order to reduce the risk of data compromise and inconsistency, and violation of confidentiality.

Academic Institutions are unique in the amount and type of sensitive data residing in its' networks and computers, such as Social Security Numbers (SSN), dates of birth, tuition account details, payment information, health records, grades, coursework, benefactor contributions, etc. Gaps in academic IT policy and procedures can endanger the security of this sensitive and sometimes classified information. The issue is of particular concern for Information Technology (IT) and through the maintenance and implementation of a Data Policy we can mitigate these risks. After the Data Policy is complete the IT group will complete a Disaster Recovery Plan (DRP) according to the requirements of the policy.

This data policy defines the ownership, security, privacy, and protection requirements for administrative data and applications residing on KSC computing systems and accessible by staff, faculty, and students.

A. Scope of Policy

Keene State College owns all institutional data. College data is defined as: data residing in databases resulting from college operations (primary databases); secondary databases derived from operational databases; and results of surveys and focus groups. These data are the exclusive property of Keene State College.

Campus data can be ...

- Contained in any form, including but not limited to documents, spreadsheets, databases, email, and web sites.
- Represented in any form including but not limited to letters, numbers, words, pictures, sounds, symbols, or any combination thereof.
- Communicated in any form including but not limited to handwriting, typewriting, printing, photocopying, photographing, and web publishing.
- Recorded upon any form including but not limited to papers, maps, films, prints, microfiche, discs, drives, and other devices.

B. What is covered

This policy applies only to data maintained in electronic form whose ownership resides with the college. However, the practices articulated in the policy are suggested irrespective of ownership.

Examples of data residing in databases resulting from college operations (primary databases) which are covered by this policy include but are not limited to data processed and stored in the following systems:

- Datatel Colleague which includes Admissions, Registration, Academic, Demographic, Financial Aid, Residential Life, etc. data
- Datatel Benefactor which includes alumni and fund raising data
- Judicial Database judicial related data which is only resident in this system
- Mediat Xpress system medical data which is only stored in this system (not feed from Datatel)
- Protégé counseling system counseling data which is only stored in this system (not feed from Datatel)
- ODS database disability data which is only stored in this system
- MyKSC student emails.
- Energy accounting data in the FASER Utility Energy Utilization system.
- Maintenance data in the MP2 maintenance services system.
- School data maintained in the CollegeNet Admissions web based system.
- Results of college sponsored surveys.
- Incident data stored in the AIMS Campus Safety system.
- Library data in the Innovative Interfaces Library catalog system.

Examples of data that resides in secondary databases derived from operational databases that are included in this policy includes but is not limited to data processed and stored in the following systems:

- Judicial Database student information data extracted from Datatel Colleague student information system
- Mediat Xpress system student information data extracted from Datatel Colleague student information system
- ODS database student information data extracted from Datatel Colleague student information system
- MyKSC student account information extracted from the from Datatel Colleague student information system
- Financial aide data residing in the SFS PC database.
- Faculty or other databases that is created from information available in other systems (such as Datatel).

C. What is not covered

This policy does not cover any data which is not considered to be owned by Keene State College. Since this policy is related to administrative data it does not specifically apply to academic data not considered as administrative data. For example Faculty course plans and curriculum are not covered under this policy.

In general this policy is focused on data entered into, stored in, and extracted from an electronic media. This policy is not addressing hardcopy data received by the school and stored in paper or microfiche media in office storage files.

D. Guiding Principles

The guiding principles for this policy are defined in the following:

- USNH Information Technology Security Policy available on line at <http://usnholpm.unh.edu/USY/VI.Prop/F.htm#5>

II. Data Classification

Data in general is classified as Restricted or Unrestricted Data. The following is the definition of these terms:

- Restricted Data – data that is restricted by federal or state law or school policy or data that the Data Proprietor has designated as protected from general access or modification even if such access is not prohibited by law or school policy. This data in general is considered sensitive and requires limited access and stringent security controls.
- Unrestricted Data – data that is not restricted for access by federal or state law or school policy or by the Data Proprietor.

Data can also be classified relative to the importance of the resource to the continuing operations of the school. This is referred to as Data Criticality. Data criticality can be classified into three levels as follows:

- Essential – an administrative data resource in electronic form whose loss or unavailability to the school would result in a loss in ability to perform mission critical functions.
- Required – an administrative data resource in electronic form whose loss or unavailability for an extended period of time would result in the inability to perform a non-mission critical function.

Prepared by: Data Access Policy Project Team

Approved by: CITC, May 2007

- Deferrable – an administrative data resource in electronic form that the school could function without and is not needed to correctly perform mission critical functions.

IV. Roles and Responsibilities

Each member of the school's community (Faculty, Staff, and Student) is responsible for the proper management, use, distribution, and protection of administrative data within his or her control. The following is a list of some of roles and responsibilities relative to specific data resources.

A. Administrative Officials – this category includes campus level Provost, Vice Presidents, Directors, Deans, and School Chairs who are stewards of campus data.

- Are ultimately responsible for implementing campus administrative data policy.
- Establish group procedures.
- Promote best practices for the management, use, distribution, and protection of campus administrative data based upon pertinent regulations and policies.
- Communicate these administrative data requirements and procedures to users of the data.
- Avail them and their staff of campus training resources relative to data management, use distribution, and protection.
- Insure that restricted administrative data is protected from inadvertent and or unauthorized access during transmission and downloading.

B. Campus IT Security Manager – responsible for campus compliancy to the USNH Information Technology Security Policy.

- Participates in the development, implementation, and maintenance of this Data Policy.
- Insures that the Data Policy meets the requirements of the USNH Information Technology Security Policy.
- Confirms that the roles of the Data Proprietor, Data Custodian, and Data User are assigned for essential electronic data resources.
- Provides education on the contents and or intent of the Data Policy.

C. Data Proprietor – the individuals or administrative departments with primary responsibility for determining the purpose and function of a data resource. For example Bursar, Director of Admissions, Director of SFS, Director of Residential Life.

Prepared by: Data Access Policy Project Team

Approved by: CITC, May 2007

- Grant and revoke access to the administrative data resource within their functional responsibility.
- Perform a risk analysis to determine the levels of sensitivity and criticality of the administrative data resource within their functional responsibility.
- Determine the level of security required for access controls based upon the sensitivity of the administrative data within their functional responsibility.
- Determine publishing and other distribution limitations for administrative data with a sensitive level of restriction.
- Determine business continuity requirements based upon criticality of administrative data resources within their functional responsibility.
- Determine the appropriate method for providing business continuity for administrative data resources with a critical level of essential.
- Oversee the accuracy, integrity, and integration capability of administrative data within their functional responsibility.
- Insure that restricted administrative data is protected from inadvertent and/or unauthorized access during transmission and downloading.
- Specify adequate data retention based upon government and or school policies.
- Ensure the destruction of restricted data by third party users upon completion of administrative data sharing arrangements with vendors, both internal and external to the campus.
- Ensure that administrative data is destroyed based upon guidelines and policies.
- Communicate requirements (such as use, distribution, security, business continuity, disclosure, disposal, etc.) to users of administrative data within their functional responsibility.

D. Data Custodian (includes Department Application Techs) – individuals or departments that function as the partner of the Data (Proprietor) and are responsible for the implementation of administrative primary, secondary and or tertiary data resources and the technical management of local (departmental) administrative data resources.

- Insure the data integrity of administrative data resources under their functional responsibility.
- Work with Central IT group to establish and implement standards and procedures to ensure that all administrative data resources within their functional responsibility are managed consistent with the needs and requirements of the Data Proprietor. Recommend technical solutions to Data Proprietor as needed. These procedures may include, but are not limited to, implementing business rules, following a security plan, managing the flow of administrative data, implementing changes to administrative data, executing appropriate back up procedures, and meeting data retention requirements.
- Work with Central IT group to establish and disseminate security standards and procedures for systems, applications, and administrative data following

the level of security access identified by the Data Proprietor and in accordance with the school's security policies.

- Implement security measures following the levels of access security identified by the Data proprietor, including where possible procedures that achieve audit through maintaining access and activity logs.
- Insure that restricted administrative data is protected from inadvertent and/or unauthorized access during transmission and downloading.
- Implement, at the direction of the Data Proprietor, a disaster recovery plan for administrative data resources deemed essential and for the preparation and general oversight of recovery in the event of a disaster.
- Ensure the destruction of restricted data by third party users upon completion of administrative data sharing arrangements with vendors, both internal and external to the campus.
- Ensure that administrative data is destroyed based upon guidelines and policies.

E. Campus Information Technology Group – individuals and department that provides technical support to what is generally defined as campus wide data resources. For example Campus Information Technology Department and it's associated groups such as Networking, DSS, EIS, HelpDesk; College Relations KSC Web Page Administration; Library Systems Group.

- Insure the data integrity of administrative data resources under their technical responsibility.
- Work with Departmental Application Techs to establish and implement standards and procedures to ensure that all administrative data resources within their functional responsibility are managed consistent with the needs and requirements of the Data Proprietor. Recommend technical solutions to Data Proprietor as needed. These procedures may include, but are not limited to, implementing business rules, following a security plan, managing the flow of administrative data, implementing changes to administrative data, executing appropriate back up procedures, and meeting data retention requirements.
- Work with Departmental Application Techs to establish and disseminate security standards and procedures for systems, applications, and administrative data following the level of access security identified by the Data Proprietor and in accordance with the schools security policies.
- Implement security measures following the levels of access security identified by the Data proprietor, including where possible procedures that achieve audit through maintaining access and activity logs.
- Insure that restricted administrative data is protected from inadvertent and or unauthorized access during transmission and downloading.
- Implement, at the direction of the Data Proprietor, a disaster for administrative data resources deemed essential and for the preparation and general oversight of the performance of disaster recovery in the event of a disaster.

Prepared by: Data Access Policy Project Team

Approved by: CITC, May 2007

- Ensure that when direct to destroy data that administrative data is destroyed based upon guidelines and policies.
- Perform and maintain data back-ups consistent with IT best practices.
- Insure that servers and PC storage is cleaned of data before being salvaged.
- Assist the Data Proprietor with monitoring who has what access to their data.

F. Data Integrator – individuals or departments that manage administrative data resources that integrates administrative data of two or more Data Proprietors one of which can be the Data Integrator. For example the Institutional Research department.

- Have the same responsibility for their integrated administrative data as that of the Data Proprietor. Plus the following:
- Comply with all federal and state laws and KSC policies, procedures, standards, and guidelines related to information privacy and security.
- Uphold the requirements, business rules, procedures, standards, and guidelines of the Data Proprietors from whose administrative data resources the integrated data is derived, as well as those of the associated Data Custodians, including, but not limited to, enforcing access and security requirements: ensuring the accuracy, integrity, and integration capability of the data; and protecting restricted data from unauthorized use or publication.
- Perform a risk assessment to determine the sensitivity of and associated security requirements for the newly integrated administrative data. An evaluation of the individual administrative data elements, aggregated data, and data security management should be included in the assessment.
- As a result of the assessment, institute additional access and security requirements for the integrated administrative data as needed, meeting the minimum security requirements of the original Data Proprietors at all times.
- Insure that restricted administrative data is protected from inadvertent and or unauthorized access during transmission and downloading.
- Obtain approval from Data Proprietor before using their administrative data.
- Upon initial request, fully disclose to the Data Proprietor the intended use, distribution, and medium of distribution of any administrative data deemed restricted by the Data Proprietor, and receive approval from the Data Proprietor for the intended use.

G. Data User – KSC staff, students, faculty or other individuals affiliated with KSC granted authorization to access or create campus administrative data and who use or access KSC administrative data to perform their job duties or other functions directly related to their association to Keene State College.

- Learn, understand, and comply with all Keene State College policies, procedures, standards, and guidelines governing the use of the data they are handling.

- Investigate and comply with the requirements, business rules, procedures, standards, and guidelines of the Data Proprietor as well as any technical procedures and guidelines of the Data Custodian.
- Use administrative data only in the performance of assigned duties.
- Use data for authorized purposes only.
- Accurately prepare, use, disseminate, and retain administrative data.
- Understand and follow the procedures relative to the sensitivity levels of the administrative data they are using.
- Respect the confidentiality and privacy of individuals whose records they access.
- Protect administrative data from unauthorized changes.
- Ensure that appropriate security protocols are in place when viewing, printing, transmitting, and or storing restricted administrative data.
- Insure that restricted administrative data is protected from inadvertent and or unauthorized access during transmission and downloading.
- Redistribute administrative data only with the permission from the Data Proprietor.
- Communicate the Data Proprietor's use requirements to any subsequent users.
- Report violations of campus policy and or Data Proprietor requirements to the Data Proprietor.

V. Procedures

A. Best Practices – in administering this policy, members of the campus community are encouraged to follow the best practices in this section. Departments may chose to instead follow their own established practices for managing and using administrative data as long as the practices are equal to or exceed the requirements of these practices.

1. Data Management

- a. Collect and retain only that administrative data required to perform the assigned tasks.
- b. Be aware of access rights assigned to each department individual and review and update these rights annually.
- c. Keep an inventory of administrative data systems within each department and review and update annually.
- d. When handling restricted administrative data check with the appropriate Data Proprietor to determine training requirements for access, use, and or distribution of data.
- e. To insure as much as possible accuracy, integrity, and integration in secondary and tertiary administrative systems:
 - i. Update the data in each system with data of record.
 - ii. Update data periodically by reconciling it with the data of record.

- f. Restricted and essential administrative data maintained in secondary and tertiary systems must be backed up periodically.
- g. When hiring and or reassigning individuals insure that they are trained and are knowledgeable of campus as well as specific Departmental data Policies.

2. Restricted Data

- a. Systems (departmental as well as central) should not include restricted administrative data unless absolutely necessary.
- b. Avoid transferring or storing restricted administrative data. If restricted data must be stored or used, provide as secure an environment as possible, following school security requirements established by the Data Proprietor.
- c. Avoid storing restricted administrative data on transportable equipment and external storage devices. If restricted administrative data must be transported on such devices, provide at minimum the same level of security as the school does in all areas where the equipment will be used.
- d. Do not email restricted administrative data either in the body of an email or as an attachment. Email is not a secure form of communications. Additionally the email recipient may have a less than secure computer or may elect to forward the information to another person which should not receive the restricted data.
- e. Never leave restricted administrative data exposed on unattended computer screens or leave computer screens unattended without appropriate screen access controls (such as password protected screen savers).
- f. Remove documents with restricted administrative data from printers immediately. Store documents with restricted data in locked cabinets and shred these documents when no longer required.
- g. Delete personal administrative data from systems when no longer required.
- h. Provide staff access to restricted administrative data only on a need to know basis.
- i. When restricted administrative data is included in the distribution of data to other users notify them of that fact as well as reference the applicable policies and regulations.

3. Administrative Data of Record and Unofficial Data

- a. When designing or implementing secondary or tertiary systems use data of record to populate the system
- b. When referencing or planning to reference administrative data of record, inform the Data Proprietor of the data of record. Once

- data of record is extracted for use in a systems where modification is possible it can no longer be considered data of record and become unofficial data in the secondary system.
- c. Refresh administrative data in reference system from the data of record on a regular basis.
 - d. When using unofficial administrative data for analysis and reporting note any use of unofficial data and be prepared to reconcile finding back to data of record.
 - e. Never report unofficial data as data of record.
 - f. To improve the accuracy and consistency of the administrative data across school systems communicate modifications, additions, and deletions of unofficial data related to data of record to the responsible Data Proprietor of the System(s) of Record. The responsible Data Proprietor of the System(s) of Record can then assess the changes to determine whether the data of record should be changed accordingly.
 - g. Bring errors in data of record to the attention of the responsible Data Proprietor of the System(s) of Record.

4. Computer Security

- a. Computers, whether or not desktops, laptops or servers that house restricted administrative data should be administered by professional system administrators. All computer devices should be secured in accordance with school security policies and standards (go to <http://www.keene.edu/it/security/> for more information).
- b. Protect computer access by using strong passwords (go to <http://www.keene.edu/it/security/passwordpolicy.cfm> for more information).
- c. Lock with a password protected screen saver or log off of a computer when not in use.
- d. Maintain appropriate physical security for computing devices with restricted administrative data. Servers housing restricted data must always be kept in locked server rooms Take special care with laptops that contain restricted administrative data in the event that they are stolen or lost the restricted data could be compromised.
- e. Remove all data from old computers when replacing or disposing them. Be aware that many times erased data can be recovered from old computers unless specific measures are taken to effectively remove the data.
- f. Refer to the IT Security web page for additional information relative to data security (<http://www.keene.edu/it/security/>)

5. Systems Development (department and central databases and systems)

- a. If system development is to be done on a contractual/ outsourced basis be sure that contractor/ outsourced vendor maintains the appropriate security of the data within the system that is developed as well as during the development cycle if live data is used for testing.
- b. Restricted administrative data should never be used as a key in a new system unless absolutely necessary.
- c. Where feasible do not maintain actual data in a test or development system unless the test or development system is subject to the same access and security restrictions as the production system. Restricted administrative data should be masked on open less secure test and development systems.

6. Vendor Relationships

- a. When passing administrative data to 3rd party vendors of the school be sure to do so within the written contractual agreement (including terms and conditions) that provides, at a minimum, for all a) disallowance of disclosure by the vendor or affiliate to the vendor including subcontractors, b) the requirements that all vendors and affiliates must observe the laws and policies required by KSC for privacy and security, including federal and state laws and school policies, c) a specific plan for the destruction of restricted data upon completion of the vendors or affiliates work with KSC.
- b. Consult with the KSC Purchasing Office and possibly USNH Internal Auditors to ensure that any written agreements conform to KSC and USNH policies. See recommended Clauses for Service Provider Agreements in Attachment #1.
- c. Regularly review and update agreements with external service providers to ensure vendor compliance with KSC and USNH and Data Proprietor requirements.
- d. Insure that all vendors that provide application hosting services (ASP) agree to in writing and meet all federal, state, and schools data security and privacy requirements.

B. Special Cases

1. Survey Data

When conducting campus based surveys, surveyors should investigate whether the data they are collecting is already under the responsibility of a campus Data Proprietor. If so, surveyors are obligated to follow the

rules and requirements of that Data Proprietor. These rules and requirements may include, but are not limited to, data use, security, business continuity, disclosure, disposition, and training.

A survey may result in data elements being collected that have not been previously collected and administered by a Data Proprietor. In such cases, the surveyor becomes the Data Proprietor of those data elements only, and is accountable for performing the responsibilities associated with that role.

Surveyors must be cautious and well informed on privacy issues and various regulations and policies may apply.

2. Marketing Data

One of the primary data collection activities associated with marketing efforts is the collection of contact and personal information about individuals, or directory information. As a general rule, directory information may be used only for the purpose for which it was collected and should never be shared, or sold to other campus or off-campus entities, unless expressly authorized by the individuals whose personal information is being collected.

Campus members handling marketing data must be cautious and well informed on privacy issues.

3. Outsourced Data

Agents, vendors and affiliates, both internal and external to the campus, must follow the same rules as the Data Custodian and Data Integrator when managing and using campus data. Agents, vendors and affiliates are responsible for ensuring security of administrative data during transmission and the removal of the data at the completion of the contractual arrangement.

Only Data Proprietors or Data Custodians, with permission of the Data Proprietor, are authorized to pass administrative data to 3rd party agents, vendors, or affiliates of Keene State College. All passing of administrative data to a 3rd party agent, vendor, or affiliate must be accompanied by a written contractual agreement (including terms and conditions) that provides at minimum for a) disallowance of disclosure by the agent, vendor or affiliate to other 3rd parties including subcontractors, b) the requirement that all agents, vendors and affiliates must observe the laws and policies required of Keene State College for

privacy and security including federal and state laws and campus policies, c) a specific plan by the agent, vendor and affiliates for the implementation of logical, physical, and management security strategies, and d) a specific plan for the destruction of restricted data upon the completion of the agents, vendors or affiliates work with KSC.

Consult with KSC Purchasing and possibly USNH Internal Auditing when writing an agreement for the sharing of administrative data with agents, vendors, or affiliates.

4. Office and or Function Specific Data Bases/ Systems

There is particular concern for the implementation and management of office and or function specific databases/ systems security, accuracy, and privacy. With the ready access of data to Staff and Faculty it is relatively easy to set-up stand alone databases and systems for reporting, tracking, or a range of other uses.

College personnel setting up these data bases/ systems are responsible for the management, security, accuracy, and privacy of this data as defined in government and College policies.

These databases/ systems while not necessarily wrong are a real source of concern for many reasons:

- Since the data may have come from systems of record at one point in time there are usually no assurances that the information is maintained current. Whenever this data is used it should include a statement that this is unofficial data and not the official data of Keene State College. As such the school is not responsible for the accuracy of this information.
- Since these data bases/ systems may be setup by individuals to meet the individuals needs they may not be adequately secured to insure access is limited, restricted data is not easily compromised, and data is used and distributed according to the requirements of the Data Proprietor.

The best means of minimizing this risk is through training and monitoring as well as to encourage any staff or faculty considering setting up these types of database or systems to discuss it with the Data Proprietor(s). There may be other ways to get this information and or the Data Proprietor may arrange to provide the information when needed.

VI. Policy Implementation

A. Training

It is the goal of Keene State College to provide adequate training for the proper management, use, distribution, and protection of administrative data. Administrative Officials must learn of school resources for training related to administrative data management, use, distribution, and protection and avail themselves and their staff of these resources as they become available.

This policy is itself a training document and shall be made readily available to all affected staff. Availability may be either in electronic for or paper.

Data Proprietors may establish specific training requirements as a condition of access to restricted administrative data within their area of responsibility. In such cases training shall be provided by the Data Proprietor. Administrative Officials must ensure that data users within the Administrative Official's area of supervision participate in Data Proprietor sponsored training when applicable (such as FERPA training for access to and use of student data).

Information about school data training opportunities related to data management within the Datatel Student Information System (Colleague) is available at <http://www.keene.edu/it/helpdesk/training/> .

B. Enforcement

1. Who and how

Any person who identifies what they believe is a violation of this policy must refer the violation to their immediate supervisor. The immediate supervisor must verify the violation including discussing the situation with the person accused of the violation.

Consult with the Keene State College Human resources Department on the violation and any planned corrective action.

2. Violation of Policy and Misuse of Data

Violations of this policy include, but not limited to: accessing administrative data to which the individual has no legitimate right; enabling unauthorized individuals to access administrative data; disclosing data in a way that violates applicable policy, procedure, or other relevant regulations or laws; inappropriately modifying or destroying data;

Prepared by: Data Access Policy Project Team

Approved by: CITC, May 2007

inadequately protecting restricted data; or ignoring the explicit requirements as defined by established College policy for the proper management, use distribution, and protection of data resources. Violations may result in network removal, access revocation, corrective action, and/or civil or criminal prosecution. Violators may be subject to disciplinary action up to and including dismissal or expulsion, pursuant to school policies, collective bargaining agreements, codes of conduct, or other instruments governing the individual's relationship with the school. Recourse shall be available under the appropriate section of the employee's personnel policy (USNH Personnel Policy USY V.C.8. Performance Issues) or contract, or by pursuing applicable legal procedure.

Under any conditions, consult with KSC HR Department before taking any action.

3. Arbitration of Disputes

Disputes may arise in the course of managing, sharing, and using school data, including issues of proprietorship, denial of access, misuse, etc.

Disputing parties are encouraged to make every effort to work cooperatively to reach an agreement. This includes referring the dispute to the appropriate Administrative Officer and or Data Proprietor.

VII. Glossary

<u>Term</u>	<u>Definition</u>
Administrative Officials	This category includes campus level Provost, Vice Presidents, Directors, Deans, and School Chairs who are stewards of campus data.
Campus IT Security Coordinator	Individual designated by KSC as responsible for campus compliancy to the USNH Information Technology Security Policy
Campus Wide Information Technology	Individuals and department that provides technical support to what is generally defined as campus wide data resources. For example Campus Information Technology Department and it's associated groups such as Networking, DSS, EIS, HelpDesk and College Relations KSC Web Page Administration.
Data Criticality	A measure of the importance of a data resource to the continuing operation of KSC. The criticality of a data resource determines whether or not it must be included in the schools Disaster Recovery Plan. Data criticality is classified into the following three categories: Essential, Required, Deferrable.
Data Custodian (includes Department Application Techs)	Individuals or departments that function as the partner of the Data Proprietor and are responsible for the implementation of administrative primary, secondary and or tertiary data resources and the technical management of local (departmental) administrative data resources
Data Integrator	Individuals or departments that manage administrative data resources that integrates administrative data of two or more Data Proprietors one of which can be the Data Integrator. For example the Institutional Research department.
Data of Record	Data recognized by the school as containing official information about a certain data type that users must reconcile when producing official or external to the department reports. Data of record normally resides in the System of Record, which may or may not be the place in which the data originated. Data of Record should be modified only with the consent of the Data Proprietor and only within the System of Record where the data officially resides. Data of Record is required to be maintained, accurate, and timely. School secondary and tertiary systems should use the Data of Record

<u>Term</u>	<u>Definition</u>
	whenever possible and refresh data from the System of Record on a regular basis.
Data Proprietor	This category includes campus level Vice Presidents, Directors, Deans, and School Chairs who are stewards of campus data.
Data Sensitivity	A risk characteristic used to access the level of access and security controls required to protect the data. Data falls into two levels of sensitivity: Restricted or Unrestricted.
Data User	KSC staff, students, faculty or other individuals affiliated with KSC granted authorization to access or create campus administrative data and who use or access KSC administrative data to perform their job duties or other functions directly related to their association to Keene State College.
Deferrable Data Resource	A data resource that the school could operate without; it need not be performed correctly or on schedule and would not affect mission critical business functions.
Essential Data Resource	A data resource whose failure to function correctly and on schedule could result in either a major failure to perform critical business functions, a significant loss of funds, or a significant liability or legal exposure.
Locally Administer Data Systems	Computer systems or data bases of any size, application, or platform designed, developed, and or administered in KSC departments or units other than central administrative computing systems (IT - EIS).
Mission Critical Application	Any application that is critical to the proper running of a business. If this application fails for any length of time you may be out of business.
Office of Record	The office designated by the campus as having responsibility for responding to formal requests, meeting reporting requirements, responding to audit, etc. for specific types of data.
Personal Information	Any information that identifies or describes an individual, including, but not limited to, His/her Name, social security number, physical description, home address, home telephone number, education, financial matters, medical or employment history. It includes statements made by or attributed to the individual. Not all personal information is Restricted data. To clarify whether specific information is restricted, contact the Data Proprietor of the information.
Required Data Resource	A data resource that performs an important function, but the operation of the school could continue for some designated period of time without it.

Prepared by: Data Access Policy Project Team

Approved by: CITC, May 2007

<u>Term</u>	<u>Definition</u>
Restricted Data	Administrative data which use is restricted by federal or state laws or school policy; or data that a Data Proprietor has designated as protected from general access or modification, even if such access may not be prohibited by federal or state laws or school policy. Types of restricted administrative data include, but are not limited to, data that identifies or describes an individual and data to which unauthorized access, modification, distribution, or loss could seriously or adversely affect KSC, its partners, or the public.
System of Record	An application or system formally designated and used to provide official campus information for reporting and other purposes.
Unrestricted Data	Administrative data to which access or modification is not restricted by federal or state laws or school policy and which is permitted by the Data Proprietor.

VIII. Related Documents

A. Federal Regulations

1. Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) <http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
2. Freedom of Information Act (FOIA) <http://www.usdoj.gov/04foia/index.html>
3. Health Insurance Portability and Accountability Act (HIPAA) Gramm-Leach-Bliley Act (GLBA) <http://banking.senate.gov/conf/confrpt.htm>
4. US Patriot Act, <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:%5D>

B. State Regulations

1. State of California Education Code, Section 67100 et seq.
2. State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.), <http://www.privacy.ca.gov/code/ipa.htm>
3. State of California Public Records Act (Gov. Code Section 6250 et seq.)

C. USNH Policies

1. USNH Information Technology Security Policy available on line at <http://usnholpm.unh.edu/USY/VI.Prop/F.htm#5>
2. USNH Personnel Policy USY V.C.8. Performance Issues <http://usnholpm.unh.edu/USY/V.Pers/C.8.htm>

D. KSC Policies

1. A FERPA Guide for Faculty & Staff, <http://www.keene.edu/policy/ferpa.cfm>
2. Student Records (Privacy), <http://www.keene.edu/catalog/acadpolicies.cfm#30>
3. Access and Disclosure Policy for Student Education Records, <http://www.keene.edu/policy/access.cfm>
4. IT Security Web Page on Federal, State or Local Laws, <http://www.keene.edu/it/security/laws.cfm>
5. IT Security Computer and Network Use Policy, <http://www.keene.edu/it/security/cnup.cfm?&print=1>
6. Keene State College Computer And Network Use Policy (CNUP), Revised June, 1998, <http://www.cts.keene.edu/Helpdesk/policies/CNUP.html>
7. Disclosure Policy, <http://www.keene.edu/policy/disclosure.cfm>

Prepared by: Data Access Policy Project Team
Approved by: CITC, May 2007

VIII. Attachments

A. Attachment #1 – Suggested Clauses for Service Provider Agreements

A. Attachment #1 – Suggested Clauses for Service Provider Agreements

**Suggested Clauses for Service Provider Agreements from the
USNH General Counsel's Office**

Security and Protection of Confidential Information

To the extent that SERVICE PROVIDER obtains any Confidential Information (as hereinafter defined) relating to INSTITUTION'S students or employees in the course of performing this Agreement, SERVICE PROVIDER warrants and guarantees that it: (i) will not disclose the Confidential Information to any third party (including affiliated third parties) except as required by law; (ii) will maintain commercially reasonable security to prevent disclosure of the Confidential Information, such security shall be no less rigorous than SERVICE PROVIDER maintains to protect its own confidential information, and will comply with all laws and regulations concerning safeguard of consumer nonpublic personal information; (iii) will develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality of all electronically maintained or transmitted Confidential Information, and (iv) will not appropriate the Confidential Information in any way for its own use or benefit outside of the performance of this Agreement. Confidential Information means any nonpublic information provided by or through INSTITUTION, in any form or media, that is personally identifiable, proprietary or confidential to INSTITUTION'S students, students' parents, students' spouses, alumnae or employees, including, but not limited to Covered Financial Information (as hereinafter defined). Covered Financial Information is any information that INSTITUTION has obtained from a customer (or another financial institution) in the process of offering consumers a financial product or service (e.g., consumer addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers). Within thirty (30) days following termination, cancellation, expiration or other conclusion of this Agreement, SERVICE PROVIDER shall return to INSTITUTION or, if return is not feasible, destroy all Confidential Information that SERVICE PROVIDER received from or created on behalf of INSTITUTION.

For purposes of this Agreement the following shall be deemed Confidential Information: _____

This list is not exhaustive - any information fitting the definition in the foregoing paragraph is Confidential Information regardless of whether it is included in this list.

Any breach of these provisions regarding the security and protection of Confidential Information shall constitute a material breach of this Agreement and entitles INSTITUTION to immediately terminate the Agreement without prior notice and without further obligation to SERVICE PROVIDER or penalty.

These provisions regarding security and protection of Confidential Information shall survive any expiration, cancellation or termination of this Agreement and constitute a continuing obligation of the SERVICE PROVIDER.