Holy Cross

Policies and Procedures Manual

Title:	Data Destruction
Policy Administrator:	Director of Information Technology Services
Effective Date:	Mar-25-2009
Approved by:	Director of Information Technology Services

Purpose:

This policy explains data destruction of College data to comply with federal and state laws, ensure that data is retained for only the period necessary to conduct business, and to ensure authorized personnel dispose of or destroy data in accordance with data destruction policies and procedures.

In the event that a lawsuit, claim or administrative charge has been filed - or there exists a reasonable belief that a lawsuit, claim or charge will be filed - all relevant records, including e-mails, must be preserved and safeguarded until the litigation or proceeding has terminated and the time for all appeals has expired. With rare exception, all such documents may be subject to discovery in litigation and the destruction of such records potentially subjects the College and the individuals who take such action to court-ordered sanctions.

Policy:

1.0 Legal Requirement and Penalties

This Data Destruction Policy is intended to ensure the College's compliance with all applicable laws and regulations governing the retention and destruction of its records. Federal and state laws and regulations require the College to maintain certain types of records for particular periods. Failure to maintain such records may subject the College and/or individuals to penalties and fines or may compromise the College's position in litigation.

2.0 Documents Covered by Policy

Records, documents, email and correspondence of all kinds must be managed according to the procedures outlined in this document. This policy applies to data in any form (including paper or electronic) however or by whomever created that belong to the College or were created by College employees, including faculty, as part of their work for the College or volunteers as part of their service to the College and are classified as Holy Cross Protected or Holy Cross Sensitive data as defined in the Holy Cross Data Classification Policy and Procedures.

3.0 Responsibilities

It is the responsibility of each Department to destroy the data that it originates or receives in accordance with this Data Destruction Policy.

Departments that maintain College data are responsible for establishing appropriate data management procedures and practices. Each department's administrative manager or a designee must:

- Be familiar with the College's data retention policy;

- Develop the department's and/or office's data management procedures and practices, consistent with this policy;
- Educate staff within the department in understanding sound data management practices;
- Restrict access to Holy Cross Protected and Holy Cross Sensitive data and information; and
- Coordinate the destruction of data as provided in the applicable procedures.

Data Disposal Policy

1.0 Holy Cross *Protected* and *Sensitive* Data

Electronic documents

All storage media, such as computer hard drives, flash drives, or CD/DVDs, containing Holy Cross Protected or Sensitive data in electronic form should be sent to the ITS Help Desk for secure deletion. The ITS Help Desk, under guidance of the Security Information Officer, will delete the Holy Cross Protected or Sensitive data from the media in accordance with current ITS Secure Deletion procedure. Any media which cannot be processed according to this standard will be destroyed; either smashed or degaussed, by the ITS Security Information Officer or his/her representative.

Since there is no way to know exactly what data is stored on computers used at the College, all computers will be considered to contain Protected data. All computers must have all attached electronic storage media erased prior to redeployment or disposal.

Paper documents

All Holy Cross Protected and Sensitive data existing in paper form must be disposed of by shredding. All documents should be dropped off in designated containers. Contents will be shredded by a licensed and bonded document destruction company. If a department does not have access to designated shredding containers, the department head or his/her designee shall contact Purchasing to arrange for shredding services or to purchase an individual shredder that meets or exceeds the Shredder Standards set below.

Documents taken outside of Holy Cross

Any paper or electronic documents containing Holy Cross Protected or Sensitive data taken outside of Holy Cross by employees, student workers, consultants or agents of Holy Cross must be returned to Holy Cross for proper disposal as outlined above. Any paper or electronic documents containing Holy Cross Protected or Sensitive data that are taken outside of Holy Cross by parties who are contractually bound to handle data produced by Holy Cross must dispose of paper documents through a bonded and licensed document destruction company and electronic documents through a method that meets or exceeds the standards in the Holy Cross Secure Deletion standards. Alternatively, the documents can be returned to Holy Cross for proper destruction.

2.0 Holy Cross Public Data

Paper documents

Should be recycled when possible.

Procedures:

1.0 Authorization of Destruction

Data shall be reviewed to verify that the retention period for the data in question has been properly reached. All known audits and audit discrepancies regarding data scheduled for destruction must be settled before the records can be destroyed; all known investigations or court cases involving said data must be resolved before the records can be destroyed.

Departments will record that the data was destroyed, the date of destruction, and method of destruction. Methods of destruction for specific data types must comply with the Data Destruction Policy.

2.0 Digital Data Destruction Procedures

All digital assets to be eradicated must use a 7-pass system that meets or exceeds DoD standards.

- Current practice is to use “killdisk” with 7 passes to eradicate media containing Holy Cross Protected Data.
- Current practice is to use “killdisk” with 1 pass to eradicate media containing Holy Cross Sensitive Data.

3.0 Shredder Methods

All shredders used to dispose of Holy Cross Protected data should meet the following standards:

- Type of cut: Shredders should be cross-cut or confetti-cut shredders; however, Strip-cut shredders are permitted so long as they produce volume over 50 pages or more.
- Size of cut: All shredders should produce shreds that are no larger than 5/32" by 1". Shredders that produce larger shreds are not permitted.
- Departments that will be shredding large amount of paper documents, either on a one-time basis or on an ongoing basis, should use the College's large capacity shredders located around campus or use services already provided by the College. You can contact the Purchasing office for more information on locations or services.

Frequency of Review

Reviews to determine compliance with this policy will be conducted by the Data Security Manager; or his/her designee, in accordance with The College of the Holy Cross Security Policy and Procedure Framework.

Policy adherence

Failure to follow this policy can result in disciplinary action as provided in the Employee Handbook, Student Handbook, and/or Faculty Handbook.

Questions about this policy

Questions about this policy should be directed to the Data Security Manager in ITS.

Related Information:

Holy Cross Employee Handbook
Holy Cross Student Handbook
Holy Cross Faculty Handbook
Holy Cross Data Classification Policy & Procedure
Holy Cross Secure Deletion Standards
Data Destruction Policy
Holy Cross Security Policy & Procedure Framework

Policy #	350000-005
Date of Last Review	Mar-31-2011