Haverford College
Data Management Principles

Data collection and management are critical to the success of the College's educational mission. Capturing reliable, high quality data; ensuring broad but appropriately secure access to those data; and providing sophisticated tools and techniques to enable the analysis of those data will allow the College to serve its students, alumni, and institutional stakeholders most effectively. "Data" in this instance refers to: any operational information, current or historical, about College stakeholders (including students, faculty, staff, alumni and friends, members of the Corporation and Board of Managers); academic, co-curricular and other programs; institutional finances, operations, and assets; College policies and practices; and all information related to evaluations, assessments, planning exercises, and strategic plans. The data discussed herein do not include academic research, scholarship, course materials, and other forms of intellectual property.

Haverford College follows these data management principles:

1. College data are a shared institutional asset, and individual offices are stewards of that data.

2. The College embraces collaborative and coordinated data collection, and appropriate data sharing to maximize institutional effectiveness.

    a. Data stewards have specific responsibilities for collecting, maintaining, securing, and appropriately sharing data within their purview and systems. (See Appendix I for additional detail.)

    b. The College has a process to resolve questions about appropriate access to data and the sharing of data. Data stewards who are unable to determine appropriate access to data or the sharing of data may refer the matter to the Senior Staff member(s) to whom they report for resolution. As with all administrative matters, the President may make a final determination.

    c. IITS is responsible for managing policies and protocols related to centralized and network data storage, security, and access.

    d. The College supports on-going employee technology training.

3. The College and its data stewards abide by all relevant laws and regulations. (see Appendix II for additional detail.)

Data Management Policies

1. IITS is responsible for leading the collaborative process of managing, securing, and improving our data systems. Leadership areas include:
    a. Researching, acquiring and launching institutional data systems, including initial application training and subsequent upgrades
    b. Managing the risk associated with maintaining data
        i. Developing and periodically reviewing reliable access and security controls (both technological and human) for centrally stored information, and advising data stewards on appropriate protocol for data stored in auxiliary systems.
        ii. Informing and periodically reminding all those accessing institutional data of the College's Statement on Confidentiality.
        iii. Securely maintaining centralized College records as well as those stored on network servers, and consulting with relevant data stewards and the College Archivist/Records Manager in adhering to College record retention policies.
    c. Establishing, in consultation with user groups, the systems of record and related protocols to ensure that all data-users are accessing the most accurate, up-to-date data from those systems of record; IITS responsibility includes coordination of the critical data update protocols that involve multiple departments.
    d. Facilitating employee technology training, by establishing and supporting the activities of Application User Groups (either within departments or across divisions)
2. Data stewards are responsible for ensuring the accuracy and reliability of the data within their purview.
    a. Individual offices are responsible for adhering to and periodically reviewing College policies on confidentiality.
    b. Individual offices are responsible for updating the system of record (or alerting the data steward for that system of record) of any updated information they receive.
    c. Individual offices are responsible for providing appropriate/necessary intra-institutional access to systems of record, with the assistance of IITS.
    d. Individual offices are responsible for engaging all departmental data professionals to improve data quality and processes.
    e. Individual offices are responsible for function-specific training, cross-training of staff, and documentation of local data management applications and protocols.
    f. Individual offices are responsible for securely maintaining records and consulting with the College Archivist/Records Manager in adhering to College record retention policies.
3. Application User Groups (either within departments or across divisions) support post-implementation application education and cross-training.
    a. On-going user support/troubleshooting
    b. Demonstration and sharing of techniques for accessing data within legacy, auxiliary, and new data systems

Appendix I – Data Stewards and Systems of Record

Data stewards have specific responsibilities for collecting, maintaining, securing, and appropriately sharing data within their purview and systems.

Institutional Data Stewardship Areas and Associated Information:

All Administrative Departments: Department Assessment Plan (DAP) Reports and assessment data
All Administrative Division Leadership: Division Assessment Plan (DAP) Reports and assessment data.
Admissions: applicant and financial aid data
Athletics: student team membership
Budget Office: Institutional budgets; Bookstore inventory/sales data
Campus Safety: Access control data ; Incident statistics; Parking and fee data
CAPS: Student mental health records
CCPA: external job/internship info; internal job postings; fellowships info
Center for Peace and Global Citizenship: Certain internship records;
Communications: college website, press releases, official communications
Controller's Office: college financial records, vendor and purchasing records, payroll records
Dean's Office: disciplinary, co-curricular, study abroad; LIFTFAR; Accomodation records; Title IX
Dining Services: Retail inventory and sales; Meal plans
Executive Affairs: Board of Managers information
Facilities: Arboretum data; capital plans/titles/deeds; licensing/permits; faculty housing; sustainability; key data
Health Services: student medical records, insurance information
Human Resources: employee and employment records; Benefit info; Risk management;
Hurford Center: Internship information
IITS: Account information; mailing lists; IT equipment and software inventory
Institutional Advancement: Parent information; alumni data; other donor/gift/grant data; storage of longitudinal undergraduate activities; majors/minors, year of graduation, undergraduate honors awards; post-graduate studies; career information; scans of hard-copy files
Institutional Research: Institution-level dashboard and summary data; Survey response data (CIRP First Year Student, Senior, Alumni); external/peer group data; Administrative assessment plans
International Student support: Visa information
Investments Office: Endowment and other investments records
KINSC: internship information
Library: library holdings, institutional archival records, institutional repository; circ. records
Provost's Office: Academic appointments; personnel cases; internal funding data; external reviews; course evals; faculty evals; sponsorship information; Articulation agreements; faculty handbook
Registrar: student bio-demo record; academic record, including curriculum and student academic records; parent information, course/senior capstone assessment
Residential Life: Student housing, keys, and meal information

Systems of Record by Constituency (2019):

Applicants: Slate, PowerFAIDS

Students: PeopleSoft, Engage, Adirondack, Workday, Moodle, Alma, Pyramed, Nelnet, PeopleGrove

Employees: Workday, Adirondack

Parents: Raiser's Edge, PeopleSoft

Alumni: Raiser's Edge, PeopleGrove

Friends of the College: Raiser's Edge

Appendix II – Relevant Laws/Regulations/Best Practices

Following is a sample of major laws, regulations, and best practices applicable to the College. It is not comprehensive or exhaustive.

A. Privacy

1. **FERPA** (Family Educational Rights and Privacy Act) protects the privacy of student education records.

http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

2. **HIPAA** (Health Insurance Portability and Accountability Act of 1996)– HIPAA Privacy Rule provides federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information. At the same time, the Privacy Rule is balanced so that it permits the disclosure of personal health information needed for patient care and other important purposes. The Security Rule specifies a series of administrative, physical, and technical safeguards for covered entities to use to assure the confidentiality, integrity, and availability of electronic protected health information.

http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

3. **PCI (Payment Card Industry)--**The Payment Card Industry Security Standards Council web page is a valuable resource regarding the handling of cardholder information:

https://www.pcisecuritystandards.org/security_standards/index.php

"The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step. The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process -- including prevention, detection and appropriate reaction to security incidents."

4. **PII (Personally Identifiable Information)**-- An excellent overview that provides details on protecting personally identifiable information can be found at:

http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

This "Guide to Protecting the Confidentiality of Personally Identifiable Information," was written by staff at the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) and

focuses specifically on protecting PII information stored on computers. Examples of PII include but are not limited to: Name, such as full name, maiden name, mother's maiden name, or alias. Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number; Address information, such as street address or email address. Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry); Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Organizations are asked to minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission.

5. General Data Protection Regulation (GDPR)

GDPR is a set of regulations covering data protection principles, privacy, consent, security, processing, and accountability. The circumstances under which GDPR applies are complex and intersect national boundaries as well as citizenship.

https://gdpr.eu/

B. Security

1. Identify Theft (Federal Trade Commission). The FTC Red Flags Rule requires many organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs — or "red flags" — of identity theft in their day-to-day operations. **www.ftc.gov/redflagsrule**

2. Prevention and detection of Terrorism (U.S. Department of Justice). The Patriot Act authorizes the use of surveillance mechanisms and information-sharing to prevent terrorism . **http://www.justice.gov/archive/ll/highlights.htm**

3. Electronic surveillance (Federal Communication Commission). CALEA (Communications Assistance for Law Enforcement Act) enhances the ability of law enforcement and intelligence agencies to conduct electronic surveillance. **http://transition.fcc.gov/pshs/services/calea/**

4. Tracking of foreign students . The Student and Exchange Visitor Information System (**SEVIS**) is the web-accessible database for monitoring information about exchange visitors, international students and scholars subject to this program. It was established by the Department of Homeland Security, and is administered by the Student and Exchange Visitor Program (SEVP).

Article on the overlap of privacy and security:

http://www.educause.edu/ero/article/civil-privacy-and-national-security-legislation-three-dimensional-view

C. Reporting

1. Sarbanes-Oxley Act of 2002

The Act mandated a number of reforms to enhance corporate responsibility, enhance financial disclosures and combat corporate and accounting fraud, and created the "Public Company Accounting Oversight Board" to oversee the activities of the auditing profession.

http://thomas.loc.gov/cgi-bin/query/z?c107:H.R.3763.ENR:%20

2. Gramm-Leach Bliley Act of 1999

"The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data."

https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act

D. Human Subject Research Regulations

1. Haverford College Institutional Review Board Policy: https://www.haverford.edu/provost/committees-and-reports/irb

2. U. S. Department of Health and Human Services: **http://www.hhs.gov/ohrp/index.html**

Appendix III – Reporting

Haverford College data is an institutional asset to be deployed responsibly in support of the College's educational mission. The College is committed to the highest standards of accuracy in its data collection, storage, analysis, and reporting. This addendum outlines expectations related to data reporting for all College employees through General Principles and identifies responsibilities for specific roles within the College's organizational structure.

A. General Principles for Reporting

Proper Data Use: Haverford College data is an institutional asset. All members of the community are obligated to protect and appropriately use College and third-party data. Haverford College policy prohibits all who work with College data from knowingly falsifying or fabricating data. Data used for reporting must be maintained in accordance with all applicable policies concerning security and confidentiality. Source data should be deleted or destroyed only as directed by the applicable Records Management Policy. Personal use of College data, including derived data, is prohibited.

Data Definitions: To the extent practical, data definitions cite data source, specific variable name, and applicable metric methodology. Data stewards contribute to the formulation of key institutional statistics, with

the understanding that there may be multiple valid definitions appropriate to different institutional contexts (e.g., student enrollment, faculty counts).

Integrity of Reported Data: In presenting information, data reporters strive for:

- **Accuracy** -- data are free from errors
- **Completeness** -- all values are present and marked as final and/or date-stamped
- **Consistency** -- data satisfy a set of definitions or constraints that are applied and maintained in the same manner across reports
- **Reliability** -- independent users obtain consistent results when applying the same definitions or constraints
- **Timeliness** -- data are available when required, and updated as required by policies, laws, and regulations

Reporting of College Data: Users recognize that College data–and information derived from it–are potentially complex. It is the responsibility of every user to understand the data they use, and to guard against making misinformed or incorrect interpretations or intentional misrepresentations of data. When publicly reporting information that is stewarded by another department, care should be taken to ensure that the information is appropriately represented (consistent with the five principles of data integrity above) and/or reviewed by the originating data steward(s).

B. Responsibilities for Reporting

Across the institution, all data users and consumers are individually responsible for adhering to principles. Within the College organizational structure, specific departments, divisions, or groups support data stewardship and reporting. These areas include:

College Archives and Records:

- Support the College community and its Data Stewards in the appropriate archiving of College-related business and reports.
- Review and update Records Management Policies on a periodic basis.
- Advise campus records keepers on best practice for appropriate retention and destruction in compliance with records schedules.

College Communications:

- Collaborate with IITS, the Office of Institutional Research, and the Senior Staff to establish protocols for the public presentation of data via the College website and other channels.

Data Stewards (see Appendix 1):

- Document and maintain data definitions for systems of record.
- Report to various audiences on behalf of the College.
- Regularly review and improve system of record data to ensure integrity and support accurate analytics within and across systems.

Data Stewardship Council:

- Provide cross-functional leadership for the development and implementation of data-related College policies and practices.

Enterprise Data User Group:

- Coordinate data steward work to document and maintain data definitions and integrity at the system level.
- In consultation with Data Stewards, map data flows across systems of record, and negotiate variable definitions across systems.

Instructional and Information Technology Services (IITS):

- Guide the community in preparing for the next generation of data management and reporting to support institutional improvement. This would include acquiring a data storage and reporting system, managing data integration, secure storage and access, and user support.

Office of Institutional Research:

- Function as a clearinghouse for directing community members to authoritative data sources.
- Work with the appropriate Data Stewards to define how official College metrics are calculated.
- Document data source, definition, and methodology for key externally reported metrics–subject to review by the Data Stewardship Council and/or Senior Staff.
- Collaborate with Data Stewards in the articulation of key data descriptors for and within domains such as students, employees, curricular features, financial measures, etc. in order to further the understanding and use of the most appropriate data for internal decision-making.
- Report any data discrepancies and inconsistencies identified in the course of its work to the appropriate Data Steward (and Data Stewardship Council, if necessary) for resolution.
- With the College Archives, ensure the appropriate inventorying and archiving of external reports submitted by Data Stewards on behalf of the College.

Senior Staff:

- Lead the College in the continuous improvement of information utilization and reporting.
- Set specific expectations for utilization of data and reporting tied to Departmental Assessment Plans (DAPs)

Approved by Senior Staff 6/21/2013
Approved by President Daniel Weiss 7/1/2013
Revised 12/2019 by the Data Stewardship Council
Approved by Senior Staff 12/18/2019