Haverford College
Data Governance and Management: Principles and Practice

Introduction

Data Governance includes the structures, processes, and practices we use to curate our institutional data assets and provide trusted information for stakeholders and decision-makers. 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 allows the College to leverage this information to serve its students, alumni, and institutional stakeholders most effectively.

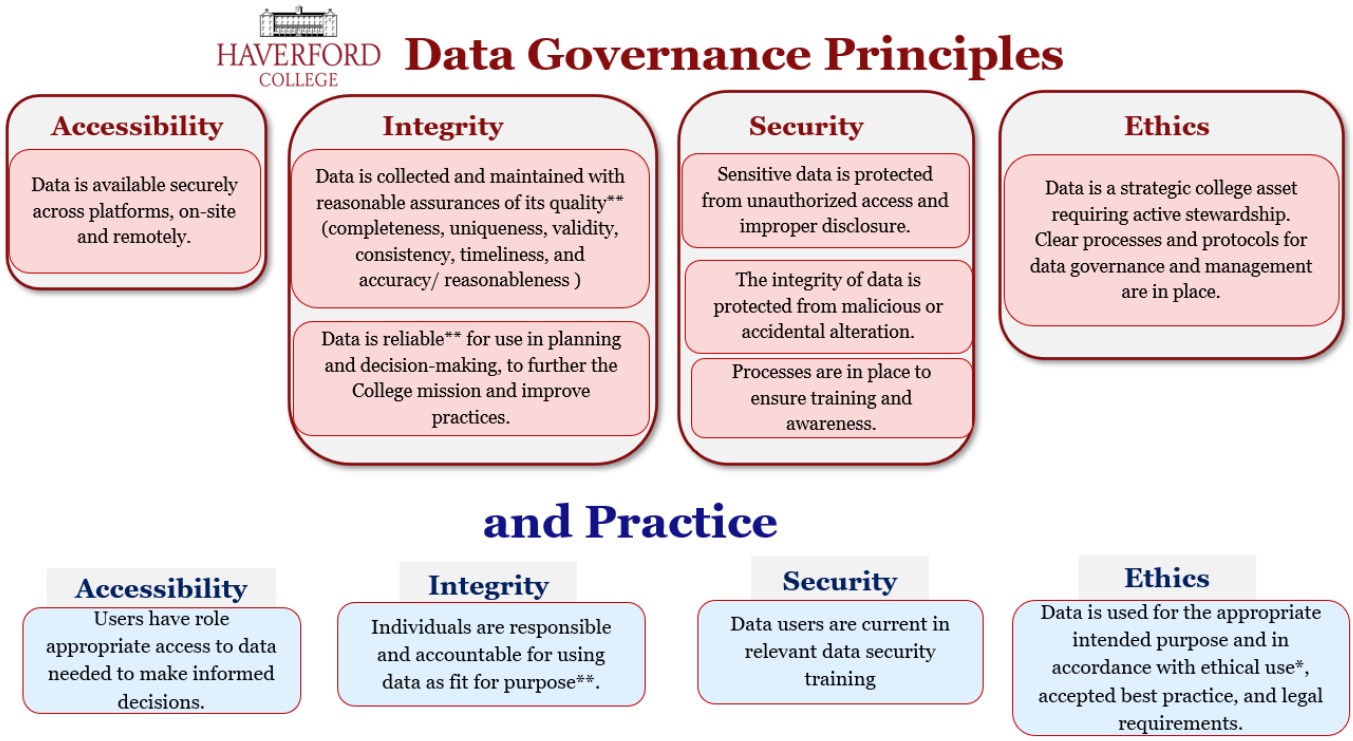
"College Data" is defined as: any operational information, current or historical, about College stakeholders (including students, faculty, staff, alumni and friends, members of the Corporation and Board of Managers); academic, co-curricular and other programs; institutional finances, operations, and 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.

In 2013, the College established three foundational data management principles:

1. College data are a shared institutional asset, and individual offices are stewards of that data. (**Appendix I-Areas of Data Stewardship Responsibility by Office/Department**)
2. The College embraces collaborative and coordinated data collection, and appropriate data sharing to maximize institutional effectiveness.
3. The College abides by all relevant laws and regulations. (**Appendix II – Relevant Laws and Regulations**)

Institutional Data Governance

In 2023, the College expanded upon the above principles with investment in technical data infrastructure, a new organizational structure for data governance, and renewed commitment to data-informed decision-making.

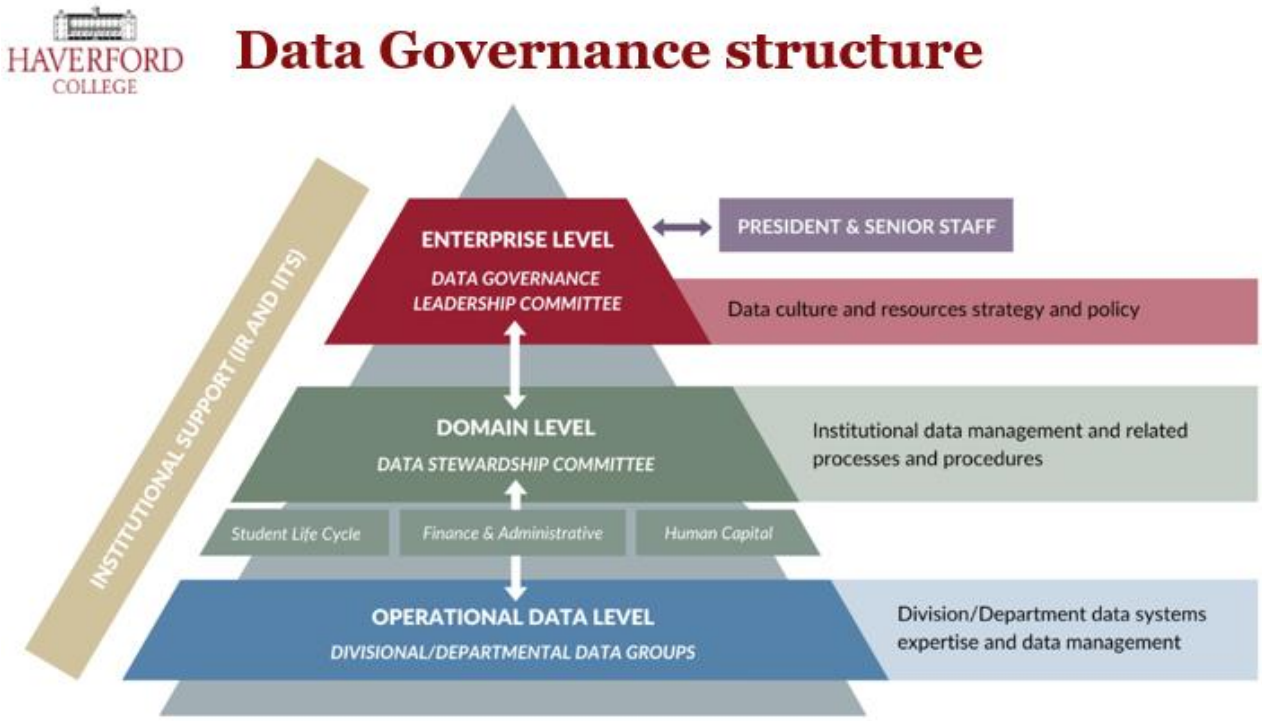


***Ethical Use of College Data**: College data–and information derived from it–are potentially complex. It is the responsibility of every data user to thoroughly understand the data they are utilizing, to guard against making misinformed or incorrect interpretations, and to prevent intentional misrepresentations of data. See Data Access and Usage Policy

**Defining Data Quality, Reliability, and Fitness for Purpose:

Completeness	All expected values, time-stamped, and adhering to defined business rules are present in the system of record.	For instance, this includes a requirement for recording a student's admission status. It also means ensuring compliance with more intricate rules, such as requiring supporting financial documentation only when a financial aid application is submitted.
Uniqueness	The degree to which data is allowed to have duplicate values.	For example, the Student ID must be unique. No two students can have the same Student ID.
Validity	The degree to which data conforms to the business rules for acceptable content within a specific College source system. This could include format, pattern, data type, valid value list, range.	Format (e.g., MM/DD/YYYY for date of birth) Pattern (e.g., numeric format for student ID) Data Type (e.g., integer for student age) Valid Value list (e.g., list of approved majors) Range (e.g., the acceptable range for SAT scores) Null Values (Exceptions have been identified where "Null" values are acceptable)
Consistency	Consistency ensures that specific data elements are uniformly defined and represented across various reports and databases within the institution.	For example, the enrollment status (full-time, part-time, Study Abroad, Deans Leave, etc.) of a student is the same across the various systems.

Timeliness	Data timeliness refers to the assurance that data are consistently available, accessible, readable, and updated across multiple systems in accordance with institutional processes, policies, and regulations.	For example, when a student updates contact information through the student portal, this change is promptly reflected in the underlying student information system and also in related systems as appropriate, maintaining consistency and accuracy of data across the institution.
Accuracy/ Reasonableness	The extent to which data aligns with known correct values, as verified by externally recognized and/or internally established sources of truth.	For instance, a student's enrollment status in an ancillary system matches the status in PeopleSoft (system of record/internal source of truth). SAT scores are within the ranges established by the College Board and within Haverford expectations.
Reliability	Reliability refers to the **consistency** and **dependability of data over time and across different contexts**. It involves ensuring that data can be consistently relied upon to produce similar results or conclusions under similar conditions.	Data is trusted and suitable for use in planning and decision-making.
Fitness for Purpose	Context, including any data anomalies are understood and taken into consideration during analysis.	For example, extensive Pass/Fail grading during the COVID global pandemic impacts analysis of student GPA data reflecting 2020-21.



Haverford College Data Governance Objectives:

- Expand data governance from a reporting systems level to an integrated College-wide approach
- Proactively identify and prioritize project opportunities to improve operational effectiveness and minimize data risks
- Champion the development and implementation of a data management solution to support information needs across the College
- Identify, catalog, and organize College data assets to enhance effective utilization enterprise-wide

- Incorporate requirements for data security, privacy, risk assessment, ethical use, and regulatory compliance.
- Ensure that data is managed in a way that supports long-term planning and decision-making by incorporating established data retention and disposal standards.
- Establish and maintain:
    - a common set of Data Governance policies, practices, and processes.
    - a cross-functional approach to overall data quality and its use in decision-making.
    - support for a set of relevant and accurate key performance indicators for the College.

The above Data Governance Program principles and objectives are carried out through three standing committees, each with a distinct focus.

1) Data Governance Leadership Committee (DGLC - red tip of the Data Governance Structure pyramid)
2) Data Stewardship Committee (DSC - green center of the pyramid)
3) Divisional Data Groups (Supporting individual Division leadership across the College- blue base of the pyramid)

HAVERFORD COLLEGE **Roles and Responsibilities**

	Enterprise Level	Domain Level Institutional Data Quality (Domains: Student Life Cycle, Finance & Admin, HCM)	Division/ Operational Level
Data Culture	Champion data culture and monitor institutional progress	Collaborate with cross-functional Stakeholders to build trusted quality data assets	Advance data utilization within the Division
Data Governance and Stewardship	Approve institutional polices and Standards	Propose and implement policies and Standards	Implement policies and standards locally
Priorities and Processes	Support the College Data Governance Program	Implement data management procedures and guidelines	Audit, clean, and identify system data gaps
Outcomes	Identify strategic enterprise-wide data opportunities/needs and desired institutional metrics	Identify, develop, monitor Domain-relevant KPIs	Identify, develop, monitor Division/ Department KPIs

Data Governance Leadership Committee (Enterprise level)

The Data Governance Leadership Committee provides strategic and comprehensive guidance for the overall care of College data assets. It empowers the enterprise-wide data governance program and supports the advancement of a culture of data-informed decision-making across the College.
The Data Governance Leadership Committee, either directly or through the work of the Data Stewardship Committee:

- Provides leadership and resources to enhance institutional data culture and infrastructure.
- Ensures that policies and standards are defined and implemented around privacy, access, security, ethical usage, regulatory compliance, and proper disposal or archiving of data.
- Supports the College's Data Governance Program to ensure that trusted data is delivered across the College.
- Communicates the importance of and expectations for adherence to data governance policy and procedures across the College.
- Advocates for the creation of additional value from College data assets, while complying with security and privacy requirements.
- Proactively prioritizes opportunities to improve operational effectiveness and minimize data risks.
- Periodically assesses the effectiveness of the Data Governance Program.

The Data Governance Leadership Committee liaises (upward) with Senior Staff as appropriate, and includes Data Stewardship Committee leadership (ex officio) for collaborative contact (downward on the Governance pyramid) with those actively managing College data resources on a regular basis. The Data Governance Leadership Committee also functions as arbiter for problems and issues that the Data Stewardship Committee is unable to resolve on its own.

Data Governance Leadership Committee Membership:

• Chief of Staff • CIO • Head of IR	• Head of IE (Ex-Officio) • Head of Data Infrastructure (Ex-Officio) • IITS Division representative(s) (Ex-Officio)

Data Stewardship Committee (Domain level)

The focus of the Data Stewardship Committee (DSC) is institutional data quality and the associated policies and processes supporting trusted data for decision makers. College data is organized into three domains which conceptually consolidate data from multiple sources: Student Life Cycle, Finance and Administrative Data, and Human Capital. Data Domain Stewards are members of the DSC as subject matter experts for our various systems of record.

Primary objectives

- Develop and propose data governance policies for Data Governance Leadership Committee consideration.
- To provide trusted data across the College, establish and steward institutional processes for :
    - Data classification(Confidential, Internal or Public as it relates to the distribution)
    - Data access (by role and a data request process)
    - Data security (including the handling of downloaded data and printed reports)
    - Data documentation (Metadata, Data Dictionary, Data Catalog, Glossary etc.)
    - Data integrity, validation, and correction (Data audit processes)
    - Data extraction and reporting
    - Data storage, retirement, and records management of exported data
- Make recommendations concerning the development and use of new institutional data to support strategic College priorities and increased effectiveness.
- Review stakeholder-proposed new technology systems for their data governance implications before purchase.
- Provide progress reports on a regular basis to the Data Governance Leadership Committee.
- Consult as necessary, including feedback on emerging dashboards

Data Stewardship Committee Membership:

• Co-Chairs
  ○ Director of Data and Analytics Infrastructure
  ○ Senior Advisor for Institutional Effectiveness
	• IITS Systems representatives (Ex Officio)
	  ○ Associate Chief Information Officer and Director of Enterprise Systems
	  ○ Director of Project Management

• Analysts (Ex Officio)
  ○ Institutional Research Analyst(s)
  ○ IT Integration and Data Specialist
	• Data Domain Stewards

Data Domain Steward: An individual appointed by Division leadership to serve on the Data Stewardship Committee based on the data responsibilities inherent in their role at the College. Appointees collaborate on College data management for one or more of the three Data Domains (Student Life Cycle, Finance/Admin, Human Capital).

- Champion the advancement of institutional data culture

- Support and actively serve as a Data Domain Steward on the Data Stewardship Committee
- Actively support data literacy skill development across the College and within the Division
- Actively encourage and support the expanded use of data in decision-making

Divisional Data Groups (Operational level)

Each Member of Senior Staff is called to actively advance data culture with the Division by supporting data fluency and expanding the use of data in decision making. This may include appointing a Divisional Data Group to advance the quality and use of data within the Division.

Primary Objectives:

- Subject Matter Expertise - Ensure that relevant data is available to support divisional effectiveness.
- Training and Documentation: Provide cross training of staff and documentation of local data management protocols and processes.
- Data Quality (within systems of record)– Ensure that data is fit for its purpose by developing data quality rules and regularly auditing data. Log data issues and work towards the resolution of data issues.Engage all departmental data professionals to improve data quality and processes.
- Data Certification – Review/revise existing reports and visualizations to ensure that they are performing as expected and meeting the needs of the Division
- Data Policies – Ensure that the Division adheres to College policy regarding privacy, access, security, ethical usage and, regulatory compliance
- Data Storage and Retention: Be responsible for securely storing and maintaining active records. Adhere to College record retention, archiving and proper disposal. Consult with the College Archivist/Records Manager as needed.

Divisional Data Group Membership:

- Appropriate Senior Staff member
- Appropriate Data Domain steward(s)
- Designated Divisional/Operational Data Manager(s)

Summary of Responsibilities

Senior Leadership (Vice Presidents directly reporting to the President): The Senior Staff is called to actively advance data culture within each Division by supporting data fluency and expanding the use of data in decision making.

Across the institution, **all data users** are individually responsible for adhering to our data principles and advancing data utilization.

Organizationally, **responsibility for constituent data quality** can be focused or shared, as outlined below:

- **Division Responsibility**: Enterprise System Content; adherence to College data policies. Primary systems by Division (2023) and constituency include:

Division	System(s) of Record	Constituencies
Academic Affairs	Peoplesoft (SIS), Workday Academic Appointment Data responsibility for faculty; Moodle (LMS), Alma (library mgmt), CourseLeaf Academic Catalog	Faculty, Students, Staff
Finance and Administration	Workday HCM (Human Capital Management), with Provost collaboration on faculty; Workday Finance, TimeClock Plus (non-exempt employee hours), CBORD (OneCard), CCURE (building access), Peoplesoft (for Student billing)	All Employees, Students
Institutional Advancement	Raiser's Edge (fundraising and constituent relationship management)	Alumni, Friends of the College, Community, Foundations/Corporations, Government.
Admission & Financial Aid	Slate (Admission) and PowerFAIDS (financial aid)	Prospective Students, Current students, Parents
Student Affairs	Engage (co-curr. records), Adirondack (housing), Maxient (conduct), Titanium (client records), Handshake (employment/career), PeopleGrove (career exploration/networking), Terra Dotta (international travel risk registry), EMS (room reservations), PyraMED (electronic medical records)	Students, Faculty, Staff
Communications	Drupal (website content management system)	Faculty, Staff, Students and External Constituents (Media, Community, Alumni, Donors)
IDEA (Institutional Diversity, Equity and Access)	none	Students, Faculty, Staff
Executive Affairs	none	Senior Leadership, Board of Managers Staff, Faculty, Students, Alumni

IITS	Qualtrics (survey data), Fischer (identity management), Box (secure document management), Google Workspace for education (email, calendar)	Students, Employees, Board of Managers

- **Division/IITS Shared Responsibility**:
  - System access approval for employees
  - Employee technical, data protocol, and content development training
  - Record retention and disposal (in collaboration with the Records Manager/Archivist)
- **IITS (Information and Instructional Technology Services) Responsibility**:
  - Researching, acquiring and implementing institutional data systems, including initial application training and subsequent upgrades
  - Maintaining information systems infrastructure; integrations between systems
  - System storage
  - Technical access protocols, security, and risk assessment
- **Institutional Data Governance Program Responsibility (DGLC/DSC leadership)**:
  - Policy development and revision
  - Other data governance activities within the scope of the DGLC/DSC's objectives
- **Data Domain Steward Responsibility:**
  - In consultation with DSC, document and maintain data definitions for systems of record
  - Regularly review and improve the system of record data to ensure integrity and support accurate analytics within and across systems
  - Report to various audiences on behalf of the College
- **College Archives and Records Responsibility:**
  - 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 Responsibility:**
  - 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
- **Office of Institutional Research Responsibility:**
  - 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
  - Report any data discrepancies and inconsistencies identified in the course of its work to the appropriate Data Steward for resolution

- **Department/Office Responsibility for Data Stewardship:** See Appendix 1

Appendix I : Areas of Data Stewardship Responsibility by Office/Department

Office/Department	Area of Stewardship Responsibility
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	Team membership and statistics
Budget Office	Institutional budgets
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 and internships
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, Bookstore inventory/sales data, student billing records
Dean's Office	Disciplinary, co-curricular; LIFTFAR; Accommodation records; Title IX; Student advising records
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; access key data

Health Services	Student medical records, insurance information
Human Resources	Employee and employment records; Benefit information
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/Effectiveness	Board and Division dashboards and summary data; Survey response data; factbook and CDS; external/peer group data; College DAP Repository; Accreditation documentation.
International Student support	Visa information
Investment Custodian	Endowment and other investments records
KINSC	Internship information
Library	Library holdings, institutional archival records, institutional repository; circ. Records, faculty publications, Senior thesis
Provost's Office	Academic appointments; personnel cases; internal funding data; external reviews; course evaluations; General Education and Capstone assessment data; faculty evaluations; sponsorship information; Articulation agreements; faculty handbook, faculty advisor records.
Registrar	Student bio-demo record; academic record, including curriculum and instructional records; parent information (relationship data/emergency contacts), EMS
Residential Life	Student housing, keys, and meal information
Risk management	Compliance tracking; institutional insurance
Study Abroad	Applications, assessments

Appendix II – Relevant Laws and Regulations

Following is a sample of major laws and regulations regarding privacy, security and reporting that are applicable to the College. It is not comprehensive nor exhaustive.

A. Privacy

1) **Family Educational Rights and Privacy Act (FERPA)**: FERPA stands for Family Educational Rights and Privacy Act of 1974 (sometimes called the Buckley Amendment) and helps protect the privacy of student education records. The Act provides eligible students the following rights:
   a) The right to inspect and review their education records;
   b) The right to request an amendment to those records if they believe there are inaccuracies or they are misleading;
   c) The right to consent to disclosure of their records;
   d) The right to file a complaint with the U.S. Department of Education.

The intention of the legislation is to protect the rights of students and to ensure the privacy and accuracy of education records. Students can be considered the "owner" of the information in their education records, and the College as the "custodian" of those records. Every institution must notify students of their FERPA rights at least annually FERPA protects the **education records** of students who are currently enrolled at Haverford or formerly enrolled regardless of their age or status with regard to parental dependency. The education records of students who have applied to but have not attended the College are not subject to FERPA guidelines, nor are the education records of deceased students.
http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

2) **Health Insurance Portability and Accountability Act (HIPAA):** – 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.
https://www.hhs.gov/hipaa/index.html

3) **Payment Card Industry(PCI)--**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) **Personally identifiable Information (PII)**
Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information

permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.
Source: https://www.dol.gov/general/ppii

4-A: Personally identifiable Information (PII) (Cyber security version): Any information about an individual maintained by the College, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf

5) The **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.
https://www.fcc.gov/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).

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.

2. **The Gramm-Leach-Bliley Act(GLBA)**

"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

3. **Human Subject Research Regulations**

   Haverford College Institutional Review Board Policy: https://www.haverford.edu/institutional-review-board-irb-human-subjects-research

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

- Approved by Senior Staff 6/21/2013
- Approved by President Daniel Weiss 7/1/2013
- Revised 12/2019 by the Data Stewardship Council
- Approved 12/18/2019 by Senior Staff as "Data Management Principles"
- Substantially revised to "Data Management and Governance: Principles and Practice," approved by Senior Staff: 12/12/2023
- Revised/Updated by DSC and approved by DGLC: 6/12/2024