HAVERFORD
COLLEGE

Policy for Handling Confidential and Internal Data
and
Acknowledgement

Introduction

Haverford College is committed to maintaining the integrity and security of confidential and internal records and information created, received, maintained, and/or stored by the College in the course of carrying out its educational mission. This policy addresses the obligations of Data End Users to secure confidential/internal information from unauthorized or unlawful disclosure. It takes into account federal and state laws governing privacy and confidentiality of records, as well as College policies and procedures addressing specific categories of records and information.

Scope

This policy applies to all employees, students, alumni, and volunteers in connection with College activities, as well as contractors, vendors, consultants, and affiliates when performing services for the College. Furthermore, it encompasses all College data (both physical and electronic) held by or on behalf of Haverford College, including data stored on College-owned or personal devices, in the cloud, or on College-owned or third-party servers.

Policy

The College expects all data End Users to adhere to safe computing and confidential data handling practices and formally acknowledge these responsibilities. These are prescribed by College and IITS policies, as well as federal and state laws. An End User is defined as anyone who views and utilizes College data. The End User is responsible for maintaining the applicable security and confidentiality of the accessed data.

Access to confidential and internal information is limited to those individuals who need it to fulfill their responsibilities. This information should only be used when necessary for business purposes. Using, accessing, or disclosing confidential, personally identifiable information (PII) or other internal data for any purpose other than legitimate job responsibilities, or in a manner that compromises the security of such information, constitutes misuse and may be illegal. Confidential and internal data must be safeguarded during use, storage, and transport. Its handling is governed by College-wide policies and internal procedures, considering legal, proprietary, ethical, business, and privacy implications.

Access and Usage

All employees and other authorized individuals (consultants and collaborators) are required to safeguard and refrain from disclosing personal account credentials that allow access to college systems in accordance with the IITS Policy on Acceptable Use of Information Technology. This policy also details procedures for any reporting violations.

The Data Access and Usage Policy provides detailed guidelines on access to confidential and internal information, as defined in the Data Classification Policy. Access is limited to individuals who require it to fulfill their responsibilities. This information must only be used when necessary for business purposes and must be safeguarded during use, storage, and transport. The policy also includes instructions on securely storing and properly disposing of physical copies of confidential and internal data to ensure ongoing protection. Authorized access to Confidential and Internal (non-public) data does not grant authorization for copying, further dissemination, or use for any other purpose than that for which the access was permitted.

Storage and Transmission

Only College-issued and secured IT resources may be used to receive, access, store, and transmit data in accordance with the requirements and safeguards of the Data Storage and Transmission Guidelines.

Acknowledgement

I will abide by these practices for Handling Confidential and Internal Data, and I understand the referenced Policies below. I will contact the IITS Security Group at hc-iits-security@haverford.edu with any questions.

- Data Classification Policy
- IITS Policy on Acceptable Use of Information Technology
- Data Access and Usage Policy
- Data Storage and Transmission Guidelines

Employees: Please acknowledge in Workday.

Outside consultants, collaborators, and others who have demonstrated a legitimate business need to handle confidential data, please acknowledge below.

Signature: ________________________________

Date: ____________________________________

Definitions

Confidential Data is that which the College must keep private:

- under federal, state, local or international laws and regulations (*see more details below for FERPA, HIPAA, GDPR, GLBA etc.)*;
- by industry standards, and/or confidentiality agreements.

Internal data is information that is proprietary or produced only for use by members of the College community who have a legitimate purpose to access such data. Its handling is based on College or department/unit protocols or procedures. Internal data generally should not be disclosed outside of the College without explicit College permission.

Non-Public Data: A Generalized term that encompasses data classified as “Confidential” or “Internal” according to the data classification matrix within the Data Classification policy. In other words any Data that is **not** classified as “Public”.

Authorized Data Personnel: An individual whose role requires access to specific data systems and responsibility for creating, altering, maintaining, securing, and appropriately reporting information.

College Data: 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.

End User: Anyone who views and utilizes College data is responsible for maintaining the applicable security and confidentiality of the accessed data.

Family Educational Rights and Privacy Act (FERPA): FERPA is a Federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children's education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level.
Source and more details: US Department of Education and FERPA

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.
Source and more details: GDPR

Gramm-Leach-Bliley Act (GLBA): 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.
Source and more details: *FTC (Gramm-Leach-Bliley Act)*

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.
Source and more details: US Department of Health and Human Services

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: *Dept of Labor*

References, Related Resources, or Appendices

First approved/Last revised January 21st, 2025
Effective date January 21st, 2025
Next review required by January 21st, 2030

Sponsors:
Megan Fitch, Chief Information Officer
Catherine Fennell, Senior Advisor to the Chief of Staff for Institutional Effectiveness
Gulal Nakati, Director of Data and Analytics Infrastructure
Contact the Office of IR and IITS with any questions.