Policy on Acceptable Use of Information Technology

Introduction

This policy addresses acceptable and unacceptable usage of College Information Technology ("IT") Resources.

Scope

This policy applies to all members of the extended Haverford College community (individually a "User" and collectively, the "Users"), including faculty, students, staff, volunteers, visitors, guests of Haverford College (the "College") and any other individual, group or entity using College IT Resources (as defined below) in any way.

Policy

A. **Intended Use**. The College provides College IT Resources for the purpose of furthering the College's mission. Limited and occasional personal use of College IT Resources is permitted to the extent that it does not interfere with institutional use.

B. **Guiding Principles**. Any use of College IT Resources must comply with all of the following:

   a. All established College policies, including Data Management Principles.

   b. All local, state, and federal laws and regulations.

   c. All license agreements, copyrights, and intellectual property laws.

C. **Prohibited Practices**. Use of College IT Resources in any of the following manners is expressly prohibited and a violation of this policy. Examples of prohibited practices are provided, but should not be construed as a comprehensive list.

   a. **Unlawful Communications**. Use of the College IT Resources for any unlawful communications including but not limited to viewing or transmitting child pornography, or sending anonymous, forged, threatening, or harassing communications.

b. **Unauthorized access**. Attempting to access, accessing, or facilitating access to any College or external IT Resource or data without authorization. Examples include: hacking or attempting to hack into College IT Resources, using College IT Resources to hack, attempt to hack, or otherwise do damage to external Resources, logging in as / impersonating another user, sharing personal or system account information, and employing scanning or other tools to locate system and network vulnerabilities.

c. **Damage to Data Integrity**. Altering or destroying data without authorization. Examples include: intentionally deleting valued email or documents without authorization, or falsifying College data to distort work or grades.

d. **Damage to Operational Integrity**. Engaging in any activity that interferes with or otherwise harms or impairs the overall operation of College IT Resources. Examples include purposeful spread of computer viruses or other malicious software, participating in a denial-of-service attack, operating wireless network equipment that interferes with the College IT Resources, installing unauthorized wiring or making unauthorized network connections.

e. **Damage to Confidentiality**. Intentional or negligent distribution of restricted data to non-authorized audiences. Unauthorized access, possession, or distribution of data that are confidential under the College's Confidentiality Policy, regarding privacy or confidentiality of student, administrative, personnel, archival, or other records.

f. **Infringement on Copyrights**. Receipt or distribution of illegal copies of copyrighted materials (a.k.a. "piracy") is a violation of both this policy and the laws of the United States (title 17, U.S. Code). Users are required to ensure they are not violating copyrights, especially via file sharing platforms such as BitTorrent, etc., which may be legitimately used, but are also common locations for illegal file sharing. Additional guidance available in the College's Copyright Resource Guide.

g. **Other**. Other prohibited practices include: Usage of College IT Resource for unauthorized commercial or for-profit activity. Representing College IT Resources as personal IT Resources for any purpose. Any other use that violates the Guiding Principles.

D. **Security**. The security of College IT Resources is a shared community responsibility.

a. Individuals entrusted with College IT Resources must take reasonable steps to protect those resources from damage or theft.

b. Users are responsible for keeping their personal IT Resources malware- and virus-free if they will be connected to College IT Resources.

c. Users are responsible for protecting their passwords and complying with the College security measures designed to protect their credentials. Users must never share their password or log another user in under their account.

d. Users may not, without specific authorization from IITS, disable or remove security or virus protection software from College IT Resources.

e. Users must follow all IITS procedures and recommendations related to the security of college equipment and data.

E. Expectation of Privacy. As a matter of practice, College IT Resources, including all data stored or passing through, are not inspected or reviewed for compliance with this or any other policy without cause. However, this is not a waiver of the College's right to do so at any time and without notice. All College IT Resources, including email accounts, remain the property of the College and users should have no expectation of absolute privacy. **Employees must adhere to the Data Confidentiality Policy & Employee Confidentiality Statement.**

F. **Legal Compliance**. The College will, when required by subpoena, warrant, or retention order, retain or release available College data to appropriate authorities. Based on the requirement of the subpoena, warrant, or order, Users may or may not be made aware of these actions.

Procedures

A. **Audit and Enforcement**. The College may, at any time and at its sole discretion, perform an audit to determine compliance with this policy. Enforcement of this policy is likewise at the sole discretion of the College, with the exception of violation notifications received from outside parties, for example, violations of copyrighted materials, where the College is obligated to take corrective action.

B. **Reporting Violations**. If, in the normal course of business, a violation of this policy is observed, the individual noting the violation shall report the observation

to their supervisor or dean, who will notify the College Chief Information Officer. Under circumstances where reporting to one's supervisor or dean is impractical or inappropriate, individuals **shall** report suspected violations to Human Resources or directly to the College Chief Information Officer.

C. **Penalties for Non-Compliance**. Individuals found to be in violation of this policy may expect to have one or more of the following actions taken depending on the nature of the violation:

- Written warning requiring immediate response and corrective action on the part of the User.
- Isolation of the violating system from the rest of College IT Resources.
- Repossession of any College IT Resources for the purposes of remediation.
- Temporary suspension of User access pending remediation.
- Other disciplinary actions, up to and including termination or expulsion.
- Report of violation to legal authorities and possible prosecution.

Definitions

College IT Resources. Any physical or virtual device, system, software or facility owned, licensed to or controlled by the College that facilitates the storage, processing, transmission or presentation of data, **and (some of, see below) the data themselves**. The College's Instructional and Information Technology Services Departments (IITS) provides certain College IT Resources to the College community. These College IT Resources include but are not limited to:

- Tablets, computers, and peripherals like displays and printers.
- Wired and wireless network, including the College's connection to the Internet and other public and private networks.
- Systems such as learning management software, financial systems, account management, e-mail and data storage, whether hosted by the College or operated by 3rd parties on the College's behalf.
- Data created, processed, transmitted, or stored on systems owned by or operated on behalf of the College, excluding intellectual property as defined by the College's Copyright Resource Guide.

HAVERFORD COLLEGE

References, Related Resources, or Appendices

None.

First approved/Last revised December 9, 2020

Effective date December 9, 2020

Next review required by December 9, 2025

Sponsor: Kathryn Giorgianni, Director of IITS Infrastructure

Contact the Office of IITS with any questions.