Contents:

1. Status, Scope and Purpose
2. Definitions
3. Policy
4. Audit; Enforcement; Risks of and Penalties for Non Compliance

Section 1.

A. Name

The formal name of this policy is Policy on the Acceptable Use of Information Technology Resources. This policy may be commonly referred to as the Acceptable Use Policy.

B. Status of This Policy

1. Draft.
2. Legal Review
4. Redraft.
5. Committee Review and Comment.
6. Legal Review
7. Accepted 8/18/2014.

C. Scope and Purpose.

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.

D. Spirit and Intent

Technology and its application are constantly evolving and changing. The intent of this policy is to acknowledge that fluidity, establish the boundaries of appropriate technology use where definable, and establish a logical framework to discern what appropriate use means as new technologies and applications appear. The spirit of this policy is to establish those boundaries and framework consistent with applicable laws and regulations, the mission of the College, the broader landscape of College policy, general academic and social community standards, respect for the reasonable privacy of others, and the general ethical and moral standards by which members of the College community discern right from wrong. Thus, this policy reflects the standards of trust and integrity that underpin our interactions with one another.

Section 2. Definitions.

A. College Information Technology (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. The College’s Instructional and Information Technology Services Department (IITS) provides certain College IT Resources to the College community. These College IT Resources are cataloged on the IITS website. This catalog is updated as the list of College IT Resources evolves. These include, but are not limited to:

- Tablets, computers and peripherals like displays and printers.
- The College’s 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 third parties on the College’s behalf.
- Data not protected under other College policies, including intellectual property policies, stored on systems owned by or operated on behalf of the College.

These, together with College IT Resources offered and maintained by other College departments through funding or staffing for which the College is responsible, comprise that to which this policy applies.

Section 3. Policy.

A. Intended Use of IT Resources. The College provides College IT resources primarily for the purpose of furthering the College’s mission, which takes priority at all times. Incidental personal use of IT Resources is permitted to the extent that it does not interfere with the institutional use of these Resources.

B. Guiding Principles. Any given use of Information Technology Resources must meet all of the criteria below to be considered an Acceptable Use.

- In compliance with all established College policies.
- In compliance with all local, state and federal law and regulations.
- In compliance with licenses and other contracts into which the College and/or the User, as applicable, has entered, as well as with the acceptable use policies of affiliated networks and systems.

C. Prohibited Practices. Use of College IT Resources in any of the following manners is expressly prohibited and constitutes a violation of this policy. For clarity, examples of each prohibited practice are included, but should not be construed to be comprehensive lists.

- Attempting to access, accessing, or facilitating access to any IT Resources, or data stored therein, without authorization or exceeding authorized access. (e.g. hacking or attempting to hack into College IT Resources, originating outside hacking attempts using College IT Resources, logging another person in to a system, sharing personal or system account credentials, “packet-sniffing” the network or scanning for network vulnerabilities, reading another person’s e-mail, privilege escalation)

- Altering or destroying data without authorization. (e.g. intentionally deleting work email or documents without authorization to do so, falsifying College data to distort work or grades)
- Engaging in any activity that interferes with or otherwise harms or impairs the overall operation of the College’s IT Resources. (e.g., spreading viruses or Trojan Horse software, participating in a denial-of-service attack, operating wireless network equipment that interferes with the College network, unauthorized wiring or attempting to create unauthorized network connections)

- Unlawful communications, including threats of violence, child pornography, and harassing communications.

- Intentional or unintentional distribution of publicly restricted data outside of the normal and customary audience of that data. (e.g. making directory listings public)

- Unauthorized access, possession, or distribution, by electronic or any other means, of data that is confidential under the College’s policies regarding privacy or the confidentiality of student, administrative, personnel, archival, or other records. (e.g., publishing student records)

- Impersonating another user. (e.g. sending an unauthorized message in another person’s name, using another person’s username and password)

- Sending anonymous, forged, threatening, or harassing communication. (e.g. spamming others, using the College network to send harassing e-mail)

- Using College IT Resources for commercial or for-profit activity that jeopardizes the College’s nonprofit status.

- Reselling IT Resources to non-College organizations or individuals.

- Intentionally infringing upon the intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction). (e.g. sharing music or movies using BitTorrent, using software for which you are not licensed, taking the academic or other professional work product of another person and representing it as one’s own)

- Any other use that does not meet the criteria in Section 3.A.

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

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

- Users are responsible for maintaining malware- and virus-free personally owned hardware and software that connects to any College IT Resources.

- Users are responsible for protecting their passwords, and changing passwords in accordance with password policy or when one suspects that their password has been compromised. Personal passwords should never be shared.

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

E. Incidental Access. IITS staff or others in the community may from time-to-time, be exposed to systems and data stored in or passing through the College IT Resources as part of the normal course of business and in the ongoing support of those resources.

- Incidental exposure to such data and systems shall be treated with the utmost discretion.

- As a matter of practice, data stored on or passing through College IT Resources are not inspected or reviewed for compliance with this or any other policy without cause.
If, in the normal course of business, a clear violation of this policy is observed as a result of incidental exposure to data or systems, the individual noting the violation shall report the observation to his or her supervisor, who then shall notify the College Chief Information Officer. Under circumstances where reporting a violation to one’s supervisor is impractical or inappropriate, individuals may report suspected violations directly to the College Chief Information Officer.

Depending on the nature of the violation, an individual may also be obligated under other College policy or law to otherwise report the observation.

F. Legally Mandated Release of Data and Records. The College will, when required by subpoena or warrant, release available data on College IT Resources to governmental authorities. Based on the requirement of the subpoena or warrant, Users may or may not be made aware of such release.

Section 4. Audit; Enforcement; Risks of and Penalties for Non Compliance

A. Audit.

IITS generally does not perform specific audits of content beyond those required as part of the normal course of business. However, nothing in this policy shall be construed as a waiver of the College’s legal rights related to College IT Resources.

IITS will, from time to time, scan the entire network for security vulnerabilities and risks to the computing environment. These scans examine every device attached to the Haverford network.

When notified of a suspected violation of law or policy, IITS will investigate to confirm or disprove the violation.

B. Enforcement.

IITS will isolate from the computing environment any system found to be in violation of this policy. IITS may take possession of any College IT Resources found to be in violation of this policy in order to remediate violations or risks. It may at times be necessary for IITS to suspend someone’s access to College IT Resources immediately for violations of this policy, pending interim resolution of the situation (for example by securing a possibly compromised account and/or making the owner of an account aware in person that an activity constitutes a violation). In the case of egregious and continuing violations suspension of access may be extended until final resolution by the appropriate disciplinary body.

IITS will report violations of law to authorities as required.

C. Risk of Non Compliance.

Violations of this policy can expose individuals and the entire College community to risks including data loss, damage to the performance and integrity of the computing environment, and legal liability.

Certain misuses of IT Resources may constitute either abuse of College resources or violation of state or federal law. Users should be aware that prosecution might occur if the law is violated.
D. Penalties for Non Compliance.

Any person who violates any provision of this policy may face sanctions up to and including termination or expulsion. Depending on the nature and severity of the offense, violations can be subject to disciplinary action through the Honor Council or disciplinary procedures applicable to faculty and staff. Violations of law carry various legal penalties independent of College sanctions.