BOARD OF TRUSTEES
UNIVERSITY OF THE VIRGIN ISLANDS

Resolution approving an Acceptable Use Policy for the University of the Virgin Islands

---

WHEREAS, it is the intention of the Board of Trustees (Board) of the University of the Virgin Islands (University) to ensure the University and its stakeholders are protected from illegal or damaging actions by individuals either knowingly or unknowingly through the use of the University's electronic resources; and

WHEREAS, the University has invested institutional resources, both monetary and human, to provide the electronic resources needed for University stakeholders to perform the business of the University and the very nature of these resources make them both valuable and limited and a privilege granted to University stakeholders; and

WHEREAS, with this privilege, the University imposes the necessary obligations and responsibilities upon its stakeholders and the University is endowing all of the stakeholders with the overall responsibility to maximize the resources and use them in an ethical and efficient way consistent with University policies and contracts, and territorial and federal laws; and

WHEREAS, on August 2, 2011, the Cabinet of the President of the University voted to recommend for consideration and approval a draft Acceptable Use Policy; and

WHEREAS, on October 12, 2012, the University Senate voted to recommend for consideration and approval by the Board the draft Acceptable Use Policy; and

WHEREAS, on May 6, 2013, the Finance and Budget Committee of the Board of Trustees voted to recommend to the Board of Trustees the approval of the Acceptable Use Policy incorporated into this resolution as "Exhibit A."

NOW THEREFORE BE IT RESOLVED AS FOLLOWS:

A. That, for the purpose of ensuring the University and its stakeholders are protected from illegal or damaging actions by individuals either knowingly or unknowingly through the use of the University's electronic resources, the Acceptable Use Policy which is incorporated into this resolution as "Exhibit A", is hereby approved.
B. That the President and Chief Information Officer are authorized to take such actions as are necessary and proper to implement this resolution.

CERTIFICATION

The Undersigned does hereby certify that the foregoing is a true and exact copy of a resolution of the Board of Trustees of the University of the Virgin Islands adopted at a meeting on June 15, 2013 as recorded in the minutes of said meeting.

Secretary of the Board

June 15, 2013
Date

Exhibit A

UNIVERSITY OF THE VIRGIN ISLANDS
Acceptable Use Policy

The University of the Virgin Islands' intention for publishing an Acceptable Use Policy is not to restrict or limit access to University electronic resources for faculty, staff or students but to ensure the University and its stakeholders are protected from illegal or damaging actions by individuals either knowingly or unknowingly.

The University of the Virgin Islands has invested institutional resources, both monetary and human, to provide the electronic resources needed for University stakeholders to perform the business of the University. The very nature and expense of these resources make them both valuable and limited and a privilege granted to University stakeholders.

With this privilege, the University imposes the necessary obligations and responsibilities upon its stakeholders. The University is endowing all of these stakeholders with the overall responsibility to maximize the resources and use them in an ethical and efficient way consistent with University policies and contracts, and territorial and federal laws. The University makes resources available to its campuses, its instructional sites and to stakeholders remotely in the expectation that these resources will be used for the purpose of performing University business in the process of achieving the mission and vision of the University. The University accepts the reality that personal calls or emails may be received and/or sent.

The expectation of acceptable use is consistent with the University's seven management values, including uncompromised integrity, fiscal responsibility, and high quality services that reflect academic honesty and shows deliberate acknowledgement of the impact of consuming scarce and shared resources. This obligation to the University dictates adherence to intellectual property policies, protection of private and personal data, respect for data ownership and copyright laws, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation, harassment or a hostile work environment. This includes viewing, downloading or storing pornography. Any actions that disregard these values demonstrate unacceptable use of the University's resources and could jeopardize access to these resources.

The "Stakeholders" covered by this policy have been given access to the University's computers, telephones, video systems, portals, Internet connections and network systems. The level of this access is based on their role in the institution as defined by their supervisors and the owners of relevant data. This access is defined in the Banner database. Receipt of a University ID number through the Banner system, based on their defined role, implies the acceptance of this policy.

The "Resources" covered by this policy include, but are not limited to:

- All University owned, operated, leased, or contracted computing, networking, telephone, videoconference technologies and e-learning information resources, whether they are individually controlled, handheld, shared, stand alone, or networked;
- All information maintained in any form and in any medium within the University's computer resources, and

- All University voice, video and data networks, email systems, telecommunications infrastructure, communications systems and services and physical facilities including all hardware, software, applications, databases and storage media. This includes telephone use and long distance access codes, all classroom equipment and all media equipment circulated from the University libraries. Personal devices that are used to access these networks and systems are also covered under this policy.
- All shared data storage resources both local and cloud-based, including storage on email servers, portal servers, and shared network drives.

By accepting access to the University's resources, all stakeholders understand and agree to the following:

- Resources shall not be used for any illegal activity or for any activity prohibited by this policy including but not limited to the items specifically listed in the following section, the Student Code of Conduct, the Faculty Policy Manual, UVI Code of Conduct and the Employee Policy Manual.
- Resources shall not be used to infringe upon or otherwise impair, interfere with or violate any copyright or other intellectual property rights of another. This pertains to all copyrighted material, including, but not limited to music, video and software licenses. Stakeholders may be potentially liable for misuse of the resources, including acts that are contrary to University policy. It is the user's responsibility to know the copyright laws, including fair use of digitized works. Users can get additional information from the University's Libraries or the Centers for Excellence in Teaching and Learning if they are unclear about the limits of use.
- Stakeholders shall avoid any action that interferes with the efficient operation of resources or impedes the flow of information necessary for academic or administrative operations of the University.
- Stakeholders shall protect their computer resources such as passwords from unauthorized use. They are responsible for reasonably securing their computer, including implementing such protections as timeouts to prohibit unauthorized use. Users are also responsible for using strong passwords and making sure they are changed on a regular basis.
- Stakeholders shall access only information that belongs to them, which is publicly available, or to which their access has been authorized by individuals or their role in Banner. They shall only access networks, network resources, and information for the intended use.
- Stakeholders shall manage shared data storage resources by limiting the amount of storage used for archived email to ten (10) gigabits per user or as may be adjusted from time to time by the University President; by archiving course information locally when asked to do so; and by abiding by storage limits on other shared systems when they are implemented.

Stakeholders are also informed by the University that:

- Electronic data, software, and communication files may be copied to backup tapes and stored for a certain period of time. Items that were deleted may be preserved on backup tapes and retrieved if necessary. This does not include all stored items nor does it absolve stakeholders from creating and maintaining a regular backup of their data and electronic communications.
- All activity on systems and networks may be monitored, logged, and reviewed by system administrators or discoverable in legal proceedings. In addition, all documents created, stored, transmitted, or received on University computers and networks may be subject to monitoring by system or telephone administrators.
- While every effort is made to ensure the privacy of University email, this may not always be possible. Communication tools such as email, network, Internet, and telephone should not be

considered private. Confidentiality cannot be guaranteed. The University reserves the right to monitor all email messages, network, Internet, and telephone connections.

- The University values academic freedom, free inquiry and freedom of expression. These privileges will not be restricted or interfered with because of the use of an electronic medium.
- The University recognizes both the value and expectation of privacy, however, some circumstances may warrant access to data and resources without the consent of the stakeholder, including:
    - When necessary to identify or diagnose systems or security vulnerabilities and problems, or otherwise preserve the integrity of the resources;
    - When required by territorial or federal law or administrative policies;
    - When there are reasonable grounds to believe that a violation of law or a significant breach of University policy may have taken place and access and inspection or monitoring may produce evidence related to the misconduct;
    - When such access to resources is required to carry out essential business functions of the University; or
    - When required to preserve public health and safety.

Examples of Unacceptable Use:

Behavior which violates this policy includes, but is not limited to:

- Accessing another person's computer, computer account, files, or data without permission.
- Using the campus network to gain unauthorized access to any computer system.
- Using any means to decode or otherwise obtain restricted passwords or access control information.
- Attempting to circumvent or subvert system or network security measures. Examples include creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system or application.
- Engaging in any activity that might be purposefully harmful to systems or to any stored information, such as creating or propagating viruses, disrupting services, damaging files or making unauthorized modifications to or copies of University data.
- Performing any act, intentionally or otherwise, that will interfere with the normal operation of telephones, computers, peripherals, or networks.
- Making or using illegal copies of copyrighted software, storing such copies on University systems, or transmitting them over University networks.
- Harassing or intimidating others via email, social networks or text messaging.
- Initiating or propagating any chain letters, items for sale or generating other email not consistent with the University’s mission and vision, unless a resource has been designated for that specific purpose.
- Initiating or facilitating in any way mass unsolicited and unofficial electronic mailing (i.e., "spamming", "flooding", or "bombing.").
- Forging the identity of an authorized stakeholder or machine in an electronic communication.
- Saturating network or computer resources to the exclusion of another's use, for example, overloading the network with traffic such as emails or legitimate (file backup or archive) or malicious (denial of service attack) activities.
- Using the University's systems or networks for personal gain; for example, by selling access to your ID or to a University system or network, by making personal toll calls or by performing work for profit with University resources in a manner not authorized by the University.
- Engaging in any other activity that does not comply with the general values presented above.

Enforcement

The University's first priority is to protect the resources, as defined above, from any event that interrupts or deteriorates operation. Any interruption in service is unacceptable to the University community and must be mitigated as quickly as possible. Information and Technology Services (ITS) will use its best efforts to contact the offending party via email, telephone, or in person to explain the problem and discuss its resolution before taking any action deemed necessary to protect the integrity of the resources. In the case of major infractions, for example those that impair others' ability to use networking and computing resources, ITS may immediately restrict systems or network access as it deems necessary to mitigate such activities. Only thereafter will ITS make a reasonable effort to contact the involved parties when these incidents occur.

Reports of alleged unacceptable use of University resources is important and taken very serious. To this end, the University will diligently investigate and take actions necessary to review files, copy logs, or review system access related to the alleged unacceptable use. University stakeholders are governed by University policies that include manuals and conduct for behavior policies for faculty, staff and students. Behavior that violates the acceptable use of University resources will be referred to the appropriate organizational unit for discipline according to these policies. In every case, the supervisor, manager or component head in conjunction with the relevant University policies will determine any misconduct. During this investigation or discipline process, it may be determined that access to any or all resources will be denied, as the discipline warrants.

Sources Used in the Development of this Document

This document is a compilation of best and standard practices and language from institutions of higher education modified to fit the specific needs of the University of the Virgin Islands. Specifically, this includes, but is not limited to:

- Acceptable Use Policy (AUP) for Computing and Networking Resources at Colorado State University, with permission by Patrick Burns, Vice President Information Technology (Colorado State University, 2011) http://www.acns.colostate.edu/Policies/AUP
- Academic Freedom and Electronic Communications, AAUP Policy Tenth Ed.2 (2004) http://www.aaup.org/AAUP/pubsres/policydocs/contents/electcomm-stmt.htm
- Acceptable Use Policy, Marquette University, with permission by Kathy Lang, Chief Information Officer (Marquette University, 2007, 2011) http://www.marquette.edu/its/about/aup.shtml