VANDERBILT UNIVERSITY AND MEDICAL CENTER

HUMAN RESOURCES POLICIES AND PROCEDURES

SUBJECT: ELECTRONIC COMMUNICATIONS

AND INFORMATION TECHNOLOGY RESOURCES POLICY

POLICY #HR-025

EFFECTIVE DATE: January 1, 2001

Revised: October/2009

POLICY

This policy is to provide guidance for the appropriate use of information technology resources[1] by Vanderbilt staff members, to ensure that these systems are used in an appropriate, productive and lawful manner in accordance with all other Vanderbilt policies. Information technology resources are provided to staff members for assistance with performing one's job responsibilities. Additionally, in some circumstances, this policy applies to communications and/or equipment not owned by Vanderbilt.

Introduction

Consistent with Vanderbilt's Acceptable Use Policy http://www.vanderbilt.edu/aup-april-2009.pdf , the guiding purpose of this policy is to ensure that the University's information technology resources are used to promote the core mission of Vanderbilt. Vanderbilt's information technology resources are to be used for their intended purposes and in a manner that protects their integrity and performance. In some circumstances, Vanderbilt may monitor online activity of staff utilizing Vanderbilt's electronic resources.

Additionally, as with any conduct outside of Vanderbilt, staff can be held accountable for conduct that negatively impacts Vanderbilt's core mission. This may include, but is not limited to, public internet and online information technology activities where staff members represent themselves as Vanderbilt employees, inappropriately share information related to Vanderbilt, and/or make inappropriate/unprofessional statements which may negatively impact Vanderbilt.

---

[1] Information technology resources include, but are not limited to, computers, telephones (including v-net), fax machines, the World Wide Web, Internet-based discussion groups, electronic bulletin board systems, electronic mail (including bulk), instant messaging systems, cell phones and text messaging, voicemail, fax, or any type of wireless transmission, etc.

GUIDELINES

I.   **Staff Member's Responsibilities**

A. Security of Information
1. Individuals using Vanderbilt's electronic resources are responsible for maintaining the security of information stored on each system. For more information, see Vanderbilt's Acceptable Use Policy http://www.vanderbilt.edu/aup-april-2009.pdf .

2. Staff may only use electronic resources for which access is approved. A staff member has the responsibility to notify his or her supervisor if he or she has access to resources that are not necessary to perform his or her job, for which the staff member's authorization has expired, is given by mistake, or is otherwise unauthorized or excessive.

3. Confidentiality of systems' accounts, passwords, personal identification numbers (PINS) and other types of authentication assigned to individual users must be maintained, protected, and not inappropriately shared. Staff may not use authentications that are not their own. Staff may not use electronic systems or equipment while signed in under another staff member's account or password unless given express authorization under extraordinary circumstances by their supervisor/manager. Responsibility for activity which occurs under a user-assigned authentication ultimately rests with the user to whom the authentication is assigned.

4. Individuals need to be aware of computer malware, such as viruses, spyware, trojans, root kits, and other destructive programs. Individuals should contact their technical support person for minimum security recommendations to prevent damage to Vanderbilt's data, equipment, and systems.

5. Vanderbilt resources must not be used by anyone to gain or attempt to gain unauthorized access to private information.

6. Deliberate or inappropriate propagation of any destructive or information gathering tools or disregard for minimum security recommendations that impact confidentiality, availability, or integrity of Vanderbilt systems and/or data, including but not limited to, viruses, keyboard loggers, packet sniffers, etc., is prohibited.

B. Communication Beyond Individual Area of Responsibility
Distribution of bulk/broadcast/mass e-mail, voice mail or fax messages beyond an individual's area of responsibility are only allowed with appropriate approvals prior to distribution.

1. University wide communications require the Vice Chancellor for Public Affairs or designee approval.

2. Communications to all staff require Chief Human Resources Officer or designee approval.

3. Communications to all University Central faculty require Provost or designee approval. Communications to all Medical Center faculty require Vice Chancellor for Health Affairs or designee approval. Communications to all faculty in a particular school or college require that school or college's Dean or designee approval.

4. Vanderbilt University Medical Center communications require Vice Chancellor of Health Affairs or designee approval.

5. Communications to students and/or house staff require the appropriate Dean of Students or the Associate Dean of Graduate Medical Education or their designee approval.

6. Safety/Security communications require Chief of Police, Director of Environmental Health and Safety, or designee approval. Safety/Security communications for the Medical Center may be sent with the approval of the designated Medical Center administrator.

7. Communications to the Medical Center during Emergency Operation Center activation may be necessary without normal approvals outlined above.

C. Other Electronic Activities

1. Vanderbilt's systems should only be used for University purposes. However, incidental personal use may be appropriate when supervisor approval has been obtained or in accordance with department guidelines.

2. Each individual is responsible for knowing his/her department's expectations for use of the University's equipment and systems.

3. No software may be downloaded or installed on Vanderbilt equipment that does not meet the guidelines established for computer privileges and responsibilities in the Acceptable Use Policy http://www.vanderbilt.edu/aup.html. Downloading of Internet software or data is prohibited when resulting in copyright infringement or excessive use of bandwidth.

4. The following is a list of uses that are inappropriate when using Vanderbilt's equipment or systems, regardless of whether that use occurs on or off work

time, at Vanderbilt or away from Vanderbilt. **This list of inappropriate uses also applies to any equipment or systems brought onto Vanderbilt property or equipment or systems while they are used in the course of Vanderbilt business**:

a. Supporting or opposing a candidate for public office. This does not include authorized lobbying efforts for causes aligned with Vanderbilt's core mission.

b. Recording sound, pictures, or video of exchanges or information relating to Vanderbilt business or employment practices without appropriate authorization, including surveillance of Vanderbilt property or recording of meetings or interactions taking place at Vanderbilt or concerning Vanderbilt business. It is inappropriate to record any conversations or exchanges of communications without the knowledge and consent of all participating persons.[2]

c. Accessing, sending, or soliciting messages or images that are sexually oriented, depict graphic violence, or which may offend or harass on the basis of race, sex, religion, color, national or ethnic origin, age, disability, military service, sexual orientation, gender identity or gender expression, consistent with the University's non-discrimination policy and Human Resources policies on Equal Opportunity and Affirmative Action http://hr.vanderbilt.edu/policies/hr-001.pdf and Anti-Harassment http://hr.vanderbilt.edu/policies/hr-002.pdf.[3]

d. Acting as a representative of Vanderbilt or acting in a way that would infer that one is a Vanderbilt representative or acting for and on behalf of Vanderbilt when not authorized to do so (e.g., contacting the media or government officials with Vanderbilt email, responding to complaints or questions about Vanderbilt business on internet discussion groups, etc.)

e. Sending, receiving, printing or otherwise disseminating proprietary data, trade secrets or other confidential information of Vanderbilt in violation of Vanderbilt policy, proprietary agreements or other contractual terms. Using Vanderbilt-owned data or work product for personal gain. Using Vanderbilt trademarks (name, logos), or branding without authorization. For more information about the scope of Vanderbilt's ownership of data and work product, see the Vanderbilt Office of Technology Transfer and Enterprise Development's

---

[2] Recording of meetings, presentations, activities or events require that staff members be notified in advance.
[3] Exceptions to this rule are staff members whose job duties include investigating matters of this nature and who must access materials as part of an investigation.

Technology Policy.
http://otted.vanderbilt.edu/about_otted/technology_policy/

f.   Operating a personal business or usurping Vanderbilt business opportunities. For more information, see the Conflict of Interest Policy http://www.mc.vanderbilt.edu/compliance/.

g.   Soliciting money or donations for unauthorized campaigns or for personal gain, a purpose not aligned with Vanderbilt, or any unauthorized solicitations. For more information see the Human Resource Solicitation Policy.
http://hr.vanderbilt.edu/policies/hr-039.pdf

h.   Email signatures, backgrounds, or taglines that have not been approved by the staff member's department. (e.g., unapproved graphics, personalized messages, etc.) Appropriate email signature content includes name, credentials, job title, department, and contact information only.

i.   Inappropriately sharing confidential information related to Vanderbilt business, such as personnel actions, internal investigations, or patient/student information.

j.   Excessive use of electronic systems ("cyberslacking") that negatively affects productivity or otherwise causes distractions to the staff member or his or her co-workers.

k.   Unprofessional communication that could negatively impact Vanderbilt's reputation or interfere with Vanderbilt's core mission, or unprofessional/inappropriate communication regarding members of the Vanderbilt community.

l.   Job advertising or recruiting activity that is not coordinated through Human Resources. All job applications or interest in staff employment must be expressed through the Human Resources job website.
http://vanderbilt.jobs/

m.   Long distance telephone charges to Vanderbilt that are not related to University business purposes. Using Vanderbilt business telephones for personal calls without authorization or beyond limits set by departmental guidelines.

n.   Any activity in violation of local, state, or federal law, including but not limited to gambling; defamatory remarks; destruction of Vanderbilt data or equipment; illegal file sharing; transportation of obscene

materials across state lines; dissemination or printing of copyrighted materials, or including articles and software, in violation of copyright law; accessing or sharing information in violation of the Heath Insurance Portability and Accountability Act (HIPAA) or the Family Educational Rights and Privacy Act (FERPA).

o. Any activity that results in a violation of any other Vanderbilt policy.

D. Inappropriate Activity on Systems Outside Vanderbilt

When using outside electronic communication systems that are accessible to others, including web logs (blogs), internet chat rooms or bulletin boards, or social networking sites, staff may not engage in the following:

1. Simultaneously identify oneself as a Vanderbilt employee and send, solicit, or display materials that are offensive, including sexually oriented material, graphic depictions of violence, or material that offends or harasses on the basis of race, sex, religion, color, national or ethnic origin, age, disability, military service, sexual orientation, gender identity or gender expression.

2. Unprofessional communication that could negatively impact Vanderbilt's reputation or interfere with Vanderbilt's core mission, or unprofessional/inappropriate communication regarding members of the Vanderbilt community.

3. Acting as a representative of Vanderbilt or acting in a way that would infer that one is a Vanderbilt representative or acting for and on behalf of Vanderbilt when not authorized to do so (e.g., contacting the media or government officials with Vanderbilt email, responding to complaints or questions about Vanderbilt business on internet discussion groups, etc.).

4. Sending, receiving, printing or otherwise disseminating proprietary data, trade secrets or other confidential information of Vanderbilt in violation of Vanderbilt policy, proprietary agreements or other contractual terms. Using Vanderbilt-owned data or work product for personal gain. Using Vanderbilt trademarks (name, logos), or branding without authorization from the Office of Trademark Licensing. http://www.vanderbilt.edu/licensing/licensing.html For more information about the scope of Vanderbilt's ownership of data and work product, see the Vanderbilt Office of Technology Transfer and Enterprise Development's Technology Policy. http://otted.vanderbilt.edu/about_otted/technology_policy/

5. Inappropriately sharing confidential information related to Vanderbilt business, including but not limited to, personnel actions, internal investigations, research material, or patient/student information. This includes sharing photos or partial information even when names of patients or students are not

used. For more information, please see privacy policies in Section IV.

6. Any activity in violation of local, state, or federal law as it relates to the staff member's employment at Vanderbilt, including but not limited to defamatory remarks; destruction of Vanderbilt data or equipment; or accessing or sharing information in violation of HIPAA or FERPA. This includes any activity that would cause Vanderbilt to not be in compliance with state or federal law.

II. Department's Responsibilities

Departments should consult with Employee Relations and their technical support person to develop appropriate departmental policies and procedures regarding information technology resources. See HR Manager's Toolbox.
http://hr.vanderbilt.edu/toolbox/index.htm

A. Departments are responsible for ensuring that individuals are assigned the appropriate level of security access to systems. This includes removing access or reducing levels of access when staff members are assigned to job roles that no longer require that level of access.

B. Upon transfer or termination of employment, supervisors should immediately initiate request to remove or transfer access to information technology resources. Departments should also follow-up to confirm access has been removed or changed.

C. Departments should communicate with their technical support person to ensure minimum security recommendations are being met in their areas.

D. Departments must define and communicate departmental expectations on personal use of equipment and systems to all new hires and all staff at least annually.

E. When appropriate, departments should centralize access for email from outside of the department to ensure continuation of customer service and other operations. For instructions on setting up a centralized email account, please see the Creating Centralized Email Account tool in the HR Manager's Toolbox.
http://hr.vanderbilt.edu/toolbox/index.htm

III. University's Right to Access Electronic Communications

Staff should not have an expectation of privacy regarding any information transmitted on Vanderbilt systems or stored on Vanderbilt systems. To the fullest extent permitted by state and federal law, the University reserves the rights to intercept, access, disclose, and use the wire and electronic communications transmitted by

University facilities or generated in the conduct of its business. To this end, the University reserves the right to:

A. Monitor computer account activities when:

1. Vanderbilt reasonably believes it necessary to do so to protect the confidentiality, integrity, and availability, of its systems and data or to protect Vanderbilt from liability;
2. There is concern that Vanderbilt's policies, state law, federal law, contractual obligations, or regulatory obligations have been, or are being, violated;
3. A user appears to be engaged in excessive activity, as defined by departmental performance expectations;
4. The law otherwise permits it; or
5. As otherwise needed or approved.

B. For staff in customer service roles, the department may monitor activity for the purpose of training, evaluation of performance and quality of service.

C. Access, preserve, copy, review or otherwise use electronic information in response to a request from the Office of the General Counsel, Vanderbilt Police, or Human Resources. Contact Employee Relations for more information and see information sheet on Electronic Information Access. http://hr.vanderbilt.edu/forms/index.htm

IV. General

A. Users should be aware that Vanderbilt electronic resources, including software such as electronic mail, are not necessarily secure or private.

B. Federal and State laws and regulations as well as VUMC policies define requirements for protection of patient health information and research health information. Users that access patient or research health information are responsible for knowing and following VUMC policies:

10-40.07 Access to Confidential Information

10-40.33 Authorization and Access to Electronic Systems and Applications

10-40.01 Confidentiality of Protected Patient Information

10-40.34 Protection and Security of Protected Health Information

10-40.35 Protection and Security of Research Health Information

10-40.32 Sanctions for Privacy and Information Security Violations

10-40.37 Electronic Messaging of Individually Identifiable Patient and Other Information

C. Additional information is also available in the Acceptable Use Policy http://www.vanderbilt.edu/aup-april-2009.pdf

D. Violation of local, state or federal laws or any University policies is inappropriate and may subject a staff member to Performance Improvement Counseling (PIC) up to and including termination of employment. Refer to Human Resources Performance Improvement Counseling Policy HR-014 http://hr.vanderbilt.edu/policies/hr-014.pdf and Human Resources Discharge Policy HR-015 http://hr.vanderbilt.edu/policies/hr-015.pdf. Staff members should immediately report any violation of this policy to their supervisor/manager or Employee Relations.

See Human Resources website for Frequently Asked Questions and Additional Guidelines. http://hr.vanderbilt.edu/index.htm

Approved by Lenon Coleman, Interim Chief Human Resource Officer

_____

Approved by Jerry Fife, Interim Vice Chancellor, Administration

_____

Approved by Jeffrey Balser, M.D, Ph.D., Vice Chancellor, Health Affairs

_____