	Human Resource Policy Employee Relations & Workplace Expectations	No. HR.ERW.18
	Title: USE OF INFORMATION AND TECHNOLOGY SYSTEMS	Page: 1 of 5
		Effective Date: 09-28-17
		Retires Policy Dated: 09-27-11
		Previous Versions Dated: 11-01-09; 01-01-98; 01-01-96

I. SCOPE:

This policy applies to (1) Tenet Healthcare Corporation and its wholly-owned subsidiaries and affiliates (each, an “Affiliate”); (2) any other entity or organization in which Tenet Healthcare Corporation or an Affiliate owns a direct or indirect equity interest greater than 50%; and (3) any hospital or entity in which an Affiliate either manages or controls the day-to-day operations of the facility (each, a “Tenet Entity”) (collectively, “Tenet”).

II. PURPOSE:


The purposes of this policy are to ensure Tenet’s technology and information systems such as voice-mail, e-mail, computers, associated computer networks, software, the Internet and other related technologies are used for business purposes only, to notify employees that they must limit personal use of these systems, to advise employees that all information stored in or transmitted through such systems, as well as the equipment itself is company property and to alert all employees of the privacy and confidentiality limitations inherent in the use of such company systems.

III. POLICY:

This policy governs the use of Tenet’s electronic mail (e-mail) and voice mail systems, Internet usage on company systems, computers, computer systems (sometimes referred to collectively as “information systems” in this policy) and software resident on any of these systems. The provisions of this policy are controlling on all matters related to employee Use of Information and Technology Systems and supersede any existing provision(s) contained in the Employee Handbook.

Computers, including portable computers, computer files, terminals, Internet-connected terminals, mobile devices, the e-mail system, the voice-mail system and software furnished to employees are Tenet property and intended for business use only, with the limited personal-use exception on page 3 below. These information systems, together with the Internet, assist Tenet in conducting business internally and externally. The equipment which makes up these systems together with the data stored in the systems, are and remain at all times, the property of Tenet whether they are located in your home, at a remote location or in the office. As such, all messages or information created, sent, received or stored in the systems as well as all information and materials downloaded into Tenet systems are and remain the property of Tenet. Employees should not use a password, access a file, or retrieve any stored communication without authorization. To ensure compliance with this policy, computer and e-mail usage may be monitored.

Tenet strives to maintain a workplace free of unlawful harassment and sensitive to the diversity of its employees. Therefore, Tenet prohibits the use of voice-mail, computers and the e-mail and Internet systems in ways that are in violation of this policy.


	Human Resource Policy Employee Relations & Workplace Expectations	No. HR.ERW.18
	Title: USE OF INFORMATION AND TECHNOLOGY SYSTEMS	Page: 2 of 5
		Effective Date: 09-28-17
		Retires Policy Dated: 09-27-11
		Previous Versions Dated: 11-01-09; 01-01-98; 01-01-96

Employees wishing to establish an official, work-related social media site must first gain approval from hospital administration. In addition, the site must comply with Tenet's Administrative policy on social media sites, AD 1.20 Social Media Policy. Employees may not use the Tenet or facility name, logo or photographs to establish official Company sites without written permission from Tenet's Communications Center or from the facility marketing/communications department.

Employees should strive to be accurate in your communications related to Tenet, and will comply will all applicable laws, including the Health Insurance and Accountability Act (HIPAA).

Examples of inappropriate use of the information systems include, but are not limited to, the following:

- A. Threatening other employees, business partners and competitors;
- B. Posting confidential or proprietary non-public information acquired in the course of employees' duties about their hospital, Tenet or its subsidiaries or any company with which their hospital or Tenet does business.
- C. Providing medical or health advice on any social media site.
- D. Publishing content related to patients and patient care including patient name, photos, diagnostic testing results/images, case information, or any information that may lead a reasonable person to be able to identify a patient.
- E. Updating or monitoring social media sites during work time unless this activity is specifically part of the employee's work duties.
- F. Tenet's policies regarding harassment, non-discrimination, retaliation and social media use apply; therefore, libelous, defamatory, maliciously false, obscene, indecent, lewd, violent, abusive, threatening, sexually harassing, discriminatory, and/or similar comments or conduct is strictly prohibited.
- G. Creating, displaying or transmitting offensive or derogatory images messages or cartoons regarding sex, race, religion, color, national original, marital status, age over 40, physical or mental disability, medical condition or sexual orientation or which in any way violate Tenet's policy prohibiting retaliation, employment discrimination and harassment in employment;
- H. Creating, displaying or transmitting "Junk mail" such as cartoons, gossip or "joke of the day" messages;
- I. Creating, displaying or transmitting "chain letters;" and

	Human Resource Policy Employee Relations & Workplace Expectations	No. HR.ERW.18
	Title: USE OF INFORMATION AND TECHNOLOGY SYSTEMS	Page: 3 of 5
		Effective Date: 09-28-17
		Retires Policy Dated: 09-27-11
		Previous Versions Dated: 11-01-09; 01-01-98; 01-01-96

- J. Soliciting or proselytizing others for commercial ventures or for religious or charitable causes. This includes “for sale” and “for rent” messages or any other personal notices.


Note that all employees have rights under the NLRA to engage in protected concerted activities including discussing terms and conditions of employment, wages or benefits or working conditions. Nothing in this policy is meant to, nor should it be interpreted to, in any way limit employee rights under any applicable federal, state, or local laws, including employee rights under Section 7 of the National Labor Relations Act, including but not limited to the right to engage in protected concerted activities with other employees for the purposes of their mutual aid and/or protection, or to improve terms and conditions of employment, such as wages and benefits. This protection includes a right to employee use of Tenet e-mail for such purposes, on non-working time, insofar as that use does not interfere with the performance of an employee’s job duties, including any patient care responsibilities.

Employees should not expect privacy with regard to Tenet’s information systems. Any communication which is private, confidential or personal should not be placed on Tenet’s information systems. Employees should expect that any e-mail or voice mail message that is created, sent or received and that any file in the computer network, in local PCs or on disks located on Tenet property may be read or listened to at any time. Tenet expressly reserves the right to intercept, read, review, access and disclose all e-mail messages, to intercept, listen to, review, access and disclose all voice mail messages and to intercept, read, review, access and disclose all computer files, including, but not limited to Internet usage and Web sites that you have accessed. Every time you use or log on to these devices you are consenting to such action. The reasons include without limitation, to investigate wrongdoing, to determine whether security breaches have occurred, to monitor compliance with policies and to obtain work product needed by other employees.

Tenet reserves the right to monitor, prohibit, restrict, block, suspend, terminate, delete or discontinue access to any official work-related social media sites without notice and at its sole discretion.

Deleting e-mail messages and computer files does not necessarily mean that there are not copies on the network or in storage or that the information cannot be retrieved. Accordingly, nothing should be written in a computer file or in e-mail that you would not put in a traditional hard copy document. Please note that it is possible that Tenet could choose to or be compelled to produce e-mail and computer files in litigation.

Tenet purchases and licenses the use of various computer software for business purposes and does not own the copyright to this software or its related documentation. Unless authorized by your Information Systems Director or Department Manager, Tenet does not have the right to produce such software for use on more than one computer.

	Human Resource Policy Employee Relations & Workplace Expectations	No. HR.ERW.18
	Title: USE OF INFORMATION AND TECHNOLOGY SYSTEMS	Page: 4 of 5
		Effective Date: 09-28-17
		Retires Policy Dated: 09-27-11
		Previous Versions Dated: 11-01-09; 01-01-98; 01-01-96

It is our policy that we acquire software through legitimate means and respect agreements concerning the use and copying of software. Employees must not borrow, “bootleg” or copy Tenet-licensed software for personal use or utilize it outside the limits of the license agreement negotiated by Tenet. You may not use any personally-acquired software on our computers without the express approval of an Information Systems Director or Department.

Security of our information systems is a priority and the responsibility of all employees. Each employee must log off the PC he or she uses when away from the PC for extended periods and at the end of each workday. Computer log-on IDs and passwords for network access, e-mail, voice mail and other applications should never be revealed to anyone unless requested by authorized Tenet personnel. Caution should be taken that such requests for user ID and password information are in fact coming from authorized Tenet personnel.

Employees should notify their immediate supervisor, the Information Services Department or any member of management upon learning of violations of this policy. The information age makes it difficult to cover every possible emerging technology adequately as to its capacity for abuse. Employees are expected to use good judgment in using any Tenet provided business tool. While not all inclusive, any breach of the guidelines, statement or spirit of this policy, unless specifically authorized in writing by an authorized manager, may result in disciplinary action up to and including termination of employment.

IV. PROCEDURE:

A. Facility Human Resources


1. Assist Supervisors and/or Administration with investigations of misuse of computers, software and networks.
2. Assist Supervisors with corrective action pertaining to the misuse of computers, software and networks.

B. Supervisors

1. Report any violations or potential problems to Administration and Human Resources for appropriate corrective action with employees.
2. Assist Administration and/or Human Resources with any investigations pertaining to misuse of computers, software and networks.

C. Employees

1. Report any violations or potential problems with communication on voice-mail, on e-mail or use of other software to the department manager, Human Resources, or Administration.

	Human Resource Policy Employee Relations & Workplace Expectations	No. HR.ERW.18
	Title: USE OF INFORMATION AND TECHNOLOGY SYSTEMS	Page: 5 of 5
		Effective Date: 09-28-17
		Retires Policy Dated: 09-27-11
		Previous Versions Dated: 11-01-09; 01-01-98; 01-01-96

2. Utilize the computer and computer networks solely for company business in accordance with this policy.

D. Enforcement

All employees whose responsibilities are affected by this policy are expected to be familiar with the basic procedures, protocols, and responsibilities created by this policy and its supporting documents. Failure to comply with this policy will be subject to appropriate performance management pursuant to all applicable policies and procedures, up to and including termination. Such performance management may also include modification of compensation, including any merit or discretionary compensation awards, as allowed by applicable law.

V. REFERENCES:

- Administrative policy AD 1.20 Social Media Policy
- Standards of Conduct
- Administrative policy 1.09 Media Relations and Public Release of Information
- Human Resources policy HR.ERW.20 Social Media Policy for Employees
- Administrative Policy AD 1.17 Fair Disclosure