1.0 PURPOSE

1.1. The purpose of this policy is to establish requirements for the acceptable use of CCHMC Information Systems.

2.0 POLICY

2.1. CCHMC Information Systems must be safeguarded by CCHMC Information System Users. Therefore, CCHMC Information System Users must comply with organizational standards for acceptable use. These standards are provided in CCHMC policies, procedures, and the *User Standards for CCHMC Information Technologies Manual*.

2.2. Prohibitions: Certain uses of CCHMC Information Systems are prohibited such as:

2.2.1. To knowingly commit, or conceal the commission of, violations of laws or regulations;

2.2.2. To knowingly commit, or conceal the commission of, fraud, waste, or abuse of any CCHMC resource;

2.2.3. Except when performed in an official, CCHMC-sanctioned capacity, use of CCHMC Information Systems to view, download, store, transmit or otherwise distribute:

- Pornographic materials;
- Materials encouraging the commission of criminal acts, including "how-to" guides;
- Defamatory, offensive, or inflammatory language;
- Statements that disparage any person or group based on race, gender, age, religion, national origin, military or veteran status, disability, sexual orientation, or other legally-protected status; and
- Inappropriate content considered harassment or which may contribute to a hostile work environment.

2.2.4. Interference with the intended functioning of CCHMC's Information Systems; and/or

2.2.4.1. Such inappropriate uses would include, but are not limited to: insertions of viruses into computer systems; tapping a network or monitoring a system or network using any software, tool, process, or device; sending e-mail "spam," or chain letters, destruction of another's files or interfering with another users' activities; use of software tools that attack IT resources, or other violations of security standards.

2.2.5. Activities and communications that may reflect unfavorably on CCHMC.

3.0 DEFINITIONS

3.1. CCHMC Information Systems: An infrastructure (including component parts) that collects, processes, uses, transmits, displays, stores, and distributes information. An infrastructure includes electronic information and technologies, associated processes (both manual and automatic), and the individuals employing such technologies or using such information.

3.2. CCHMC Information Systems Users: Any individual who accesses CCHMC Information Systems including, but not limited to Workforce Members, remote access users, consultants, temporary employees, and vendors.

4.0 IMPLEMENTATION

4.1. User responsibilities: CCHMC Information Systems are CCHMC property, as are communications, information, and data collected, stored, or transmitted via these systems. Access to these systems imposes certain responsibilities and obligations which include:

4.1.1. Responsible and professional behavior with respect to the use of CCHMC Information Systems;

4.1.2. Behavior consistent with the mission, vision, and core values of CCHMC and within activities authorized by CCHMC;

4.1.3. Compliance with applicable laws, regulations, and policies;

4.1.4. Truthfulness, integrity, and honesty in personal identification;

4.1.5. Respect for the rights, identity, and property of others;

4.1.6. Behavior that protects the security, privacy and integrity of electronic networks, electronic data and information, and electronic infrastructure and systems; and

4.1.7. Respect for the value and intended use of human and electronic resources.

4.2. Destruction: CCHMC Workforce Members must promptly and properly dispose of, sanitize, and/or destroy Confidential Information in any form (e.g., paper, electronic, on Portable Devices, etc.) when no longer useful. Refer to Medical Center Policy G-117 on records retention and the *User Standards for CCHMC Information Technologies Manual* for further information on destruction of Portable Devices.

4.3. Monitoring: Use of CCHMC Information Systems for any reason constitutes understanding of use requirements and consent to monitoring for proper system functionality and appropriate use. CCHMC Information Systems are subject to auditing and monitoring. Systems may be monitored for excessive or inappropriate personal use, criminal activity, regulatory violations, or other conditions as determined by the Chief Information Officer, Privacy Officer, Director of Protective Services, or the Assistant Vice President, Internal Audit, or their designees. Inappropriate use of CCHMC Information Systems may result in the deletion of applications or files at any time, without advance warning. Deleted applications and files may not be available for restore and include, but are not limited to, applications and files not related to a CCHMC purpose, unapproved applications, and software not purchased through approved mechanisms.

5.0 OVERSIGHT

The Chief Information Officer will periodically review and update this policy as appropriate.
Authority over this policy shall vest with the President and Chief Executive Officer.

6.0 REFERENCES

- 45 C.F.R. § 164.308

REVISION HISTORY	
Original Date	**4/20/2005**

- Reviewed: 5/12/2008
- Reviewed: 12/29/2010
- Revised: 11/14/2011 (Changed policy number from II-105 to INFO-102.)
- Revised: 8/15/2013