

ELECTRONIC COMMUNICATION DEVICES & SERVICES 513*Effective Date: 12/19/2016*

Electronic communication devices and services are provided by Cass County to assist employees in completing their work, improving their efficiency and obtaining work-related data and technology. The following policies have been established to help ensure responsible and productive computer usage.

Definitions

Electronic communication devices include desk phones, cell phones, computers, laptops and tablets, copiers, printers and other peripheral devices. Electronic communication services include local and long distance calling, voicemail, e-mail, instant messaging, software applications, tablet and cell phone apps, file storage systems such as SharePoint or OneDrive, network shared or personal drives and Internet access. This non-exhaustive list of technology devices and services is meant to include all forms of electronic communications, devices and services provided by Cass County. As new technologies are obtained and implemented by Cass County, those items will also be included in this policy.

All electronic communication devices and access to network services furnished to employees in the performance of their duties are the property of Cass County, and are intended for business use only. As a result, employees have no right to privacy for any uses, business or personal, to which they may be using the electronic communication devices and services provided to them. Cass County reserves the right to monitor at any time any and all uses of our equipment, network resources and Internet activity regardless of whether the use is personal in nature or occurs during non-working times, which includes breaks and lunch periods.

Personal Use of Electronic Devices and Services

While usage of the County's electronic communication devices and services are intended for job-related activities, incidental and occasional brief personal use may be permitted within reasonable limits. The personal use of electronic communications devices and services shall NOT be a substitute for keeping your business and personal e-mail, files, videos, movies, pictures and internet activity strictly separate. As such, all personal related email, files and digital media shall be conducted or stored on personally owned email accounts, devices or online services.

Cass County employees are strictly prohibited from using their County provided email or website addresses for their personal use to register or subscribe for any services including but not limited to any social media sites, online newsletters or journals, personal finance websites, public or private schools, religious or sporting activities, health services, household bills and utilities, hotel and travel sites or any online shopping or shipping services without prior approval from the IT Department.

Cass County strictly prohibits using our Internet services for the personal use of streaming video, audio, internet radio or music and using electronic devices or services for the storage, viewing or playing of personal pictures, videos, music and other personal files. Do not connect personal cell phones, iPods, other music players or playing of CD or DVD disks on county owned electronic devices.

The electronic communication devices and services provided to Cass County employees remain at all times the property of Cass County. To ensure compliance with this policy, Cass County reserves the right to monitor Internet traffic, and retrieve and read any data composed, sent, received or stored on devices or services. All data that is composed, transmitted, received or stored on our computer system is considered to be part of the official records of Cass County and, as such, is subject to open records disclosure to law enforcement or other third parties.

Employees must comply with all applicable laws (e.g., industry regulations, harassment laws, copyright restrictions, contractual obligations or restrictions, etc.) every time they use Cass County's electronic communication devices and services for any purpose, as well as during any occasion they may be using their own personal computer networks, systems, or equipment in ways that may directly or indirectly be associated with Cass County.

Computer Security

Employees should take all security precautions available to them and prescribed by Cass County. Employees should not attempt to bypass or disable any security precautions installed on Cass County computers. Similarly, employees shall protect the integrity of electronic communication devices and services at all times, which includes logging off or locking systems when not in use or away from your workspace.

Employees using electronic devices offsite, including home, hotels or other public locations shall take all precautions to protect County owned equipment. Employees shall maintain positive control of devices when in public locations and take necessary precautions when connecting to public Internet or Wi-Fi connections.

Employees who check out or are provided County resources for working off-site are prohibited from allowing non-employees, including family members, to use the electronic communication devices and services.

Passwords and user IDs to access any system shall not be written down or shared with other employees at any time and users shall not login to a system for the purposes of allowing another user access. This includes, but is not limited to, computers, servers, state applications, or online business accounts.

Employees shall not transfer, copy, upload or forward any County email, documents, or files to personally owned devices or services, including but not limited to, USB flash drives, portable hard drives, CD/DVD drives, personal email accounts or any online storage services such as Dropbox, iCloud, OneDrive, or Google Drive, without permission from the IT Department.

When required, employees should only send confidential, sensitive and/or proprietary information using County approved encryption or secure email methods. Similarly, when receiving emails, employees should encourage outside clients, vendors and business partners to send any confidential, sensitive and/or proprietary information using appropriate safeguards, including encryption or secure email methods.

Prohibited Usage

The following behaviors are examples of previously stated or additional actions and activities that are prohibited and can result in disciplinary action up to and including termination of employment:

- Sending or posting discriminatory, harassing, or threatening messages or images
- Using the organization's computer or services for personal gain. E-mail may not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-business matters.
- Sending or posting confidential material, trade secrets, or proprietary information outside of the organization (such information includes, but is not limited to, non-public information, internal documents, memorandums, announcements, financial information, prospect and customer lists, pricing and preferences)
- Failing to observe licensing agreements
- Engaging in unauthorized transactions that may incur a cost to the organization or initiate unwanted Internet services and transmissions
- Viewing or exchanging pornography or obscene materials
- Attempting to break into the computer system of another organization or person
- Refusing to cooperate with a security investigation or obstructing a security investigation
- Sending or posting chain letters or advertisements not related to business purposes or activities
- Using the computer for gambling of any sort
- Jeopardizing the security of the organization's electronic communications systems
- Sending or posting messages that disparage other organizations
- Passing off personal views as representing those of the organization
- Sending anonymous e-mail messages
- Using electronic devices or services, including email or Internet for the purposes of seeking other employment or preparing or posting a resume
- Loading software without permission
- Engaging in any other illegal activities
- Engaging in any other computer related activity determined by Cass County to be inappropriate or unacceptable

Cass County strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, Cass County prohibits the use of electronic communication devices and services in ways that are disruptive, offensive to others, discriminatory, obscene, threatening,

harassing, intimidating, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is not allowed. Other such misuse includes, but is not limited to, ethnic slurs, racial comments, gender-specific comments, off-color jokes, or anything that may be construed as harassment, bullying or showing disrespect for others.

Cass County 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 the software developer, Cass County does not have the right to reproduce or install such software for use on more than one computer. Employees may only use software on local area networks or on multiple machines according to the software license agreement. Cass County prohibits the illegal duplication of software and its related documentation.

The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. As a general rule, if an employee did not create material, does not own the rights to it, or has not gotten authorization for its use, it should not be put on the Internet or transmitted through the e-mail system.

Employees are required to sign an acknowledgement form for Cass County's Appropriate Use of Electronic Communication Devices and Services.

Consequences for Policy Violations

Abuse of the electronic communications devices and services provided by Cass County may result in suspension of Internet/e-mail privileges, and/or disciplinary action, up to and including termination of employment. Employees may also be held personally liable for any violations of this policy. Employees should notify their immediate supervisors or any member of management upon learning of violations of this policy.