

Category: 150

Number: 151

Subject: **EMPLOYEE INTERNET USE, EMAIL & REQUIRED TRAINING POLICY**

1. **PURPOSE:** To ensure the proper use of the County of Saginaw's computer and telecommunications resources and services by employees, independent contractors, elected officials and other computer users.
2. **AUTHORITY:** Saginaw County Board of Commissioners. Changes to this policy will be made and approved by the Board of Commissioners based on changes in technology and business practice.
3. **APPLICATION:** This policy applies to all Departments, Elected Offices and Agencies of Saginaw County.
4. **RESPONSIBILITY:** Information Technology of Saginaw County (ITSC) is responsible for the implementation of this policy.
5. **DEFINITION(S):** NONE
6. **POLICY:** This policy will establish best practices and provide guidance for Saginaw County employees to follow in an effort to better secure our network infrastructure and technology assets. Standards and related processes and procedures will be consistently developed and maintained to ensure compliance with these policies. The computers and computer accounts provided to employees are to assist them in the performance of their duties to serve the constituents of Saginaw County. Email and Internet services are available to employees and officials for conducting county business. Using these systems is a privilege, not a right. Inappropriate use will result in the loss of this privilege and/or progressive discipline up to, and including discharge.

#### 6.1 Legal Issues

6.1.1 It is illegal to intentionally access a computer system or network for the purpose of:

6.1.1.1 Devising or executing any scheme or artifice to defraud or extort.

6.1.1.2 Obtaining money, property or services with false or fraudulent intent, representations or promises.

6.1.2 It is also illegal to maliciously access, alter, delete, damage or destroy any computer system, computer network, computer program or data, using an unauthorized account, changing other users passwords, damaging files, altering the system or using the system or network to make money illegally.

- 6.1.3 It is additionally illegal to violate plagiarism and copyright laws.
- 6.1.4 Any employee committing acts of this nature will face disciplinary action according to Saginaw County policies and be subject to local, state and federal laws.

## 6.2 Enforcement

- 6.2.1 Any violation of this policy constitutes just cause for taking disciplinary action, revoking network privileges and/or initiating legal action for any illegal, inappropriate or obscene use of the network or in support of such activities.
- 6.2.2 Saginaw County and ITSC will actively monitor network activity in any form to maintain network integrity and to ensure that no illegal, inappropriate or improper activity is occurring within the Saginaw County network environment or representation of Saginaw County.

## 6.3 Roles & Responsibilities

- 6.3.1 All users are responsible for:
  - 6.3.1.1 Knowing, understanding, and following all County policies.
  - 6.3.1.2 Exercising good judgment and acting in a professional manner when using County technology resources.
  - 6.3.1.3 Upon transfer to a new assignment, requesting that the authorities assigned to their User ID be changed to reflect the access requirements of the new job.
  - 6.3.1.4 Immediately reporting security incidents such as their computer or device becoming possibly compromised or infected with any type of malicious entity.

## 6.4 Management is responsible for:

The actions of their staff, contractors, and volunteers and must ensure that all standards applicable to their environment are followed alerting ITSC via the appropriate form or a service desk ticket when a user transfers to new responsibilities. The privileges assigned to the user's ID must be changed to reflect the access requirements of the new job.

## 6.5 Employment Internet Procedures - General

- 6.5.1 All use of the Internet must be for authorized purposes. Saginaw County, through ITSC, reserves the right to prioritize use and all access to the network including sensitive data.
- 6.5.2 All use of the Internet must be in conformity with local, state and federal law and Saginaw County policies and procedures.

- 6.5.3 No statement may be made that can be construed to be "Official Saginaw County Policy" if the individual is not authorized to represent Saginaw County.
- 6.5.4 The system and network at Saginaw County constitute public facilities and as such may not be used to support or oppose political candidates or ballot measures.
- 6.5.5 Hate mail, harassment, discriminatory remarks or other antisocial behavior is prohibited and subject to termination through Personnel protocol.
- 6.5.6 Use of the system or network from Saginaw County facilities to access, view, store or distribute obscene or pornographic material is prohibited and subject to termination through Personnel protocol.
- 6.5.7 Subscriptions to mailing lists, bulletin boards, chat groups, commercial on-line services or other information related services must be previously approved by an employee's department head and ITSC and must be related to County business.
- 6.5.8 No employee will have access to the Internet without having received appropriate training and acknowledging they have read, understand and agree to this policy.
- 6.5.9 Users must identify themselves clearly and accurately in electronic communications. Anonymous or pseudo-anonymous communications appear to dissociate users from responsibility for their actions and are prohibited.
- 6.5.10 Concealing user identity or misrepresenting a user name or Saginaw County to mask or distance users from irresponsible or offensive behavior is a serious abuse of network privileges and violates Saginaw County policies and procedures.
- 6.5.11 Using identifiers of others constitutes fraud and is a violation of Saginaw County policies and procedures.
- 6.5.12 Users are cautioned that information on the Internet is from unknown sources and consequently must always be subject to verification.

## 6.6 Etiquette

- 6.6.1 Be polite and use appropriate language.
- 6.6.2 Do not reveal personal address or telephone number(s) or those of colleagues.

- 6.6.3 Do not use the network in such a way that would disrupt the use of the network by others.
- 6.6.4 All communications and information accessible via the network should be assumed to be private property.
- 6.6.5 Users are responsible for the appropriateness and content of material they transmit or publish on the network. Hate mail, harassment, discriminatory remarks or other antisocial behavior such as targeting another person or organization to cause distress, embarrassment, injury or unwanted attention is prohibited. Personal attacks or other sanctions to threaten or intimidate or embarrass an individual, group or organization or attacks based on a person's race, national origin, ethnicity, disability, religion, gender, veteran status or sexual orientation are prohibited.

## 6.7 Security

- 6.7.1 Sharing or otherwise divulging a user's password and/or account code with another person is prohibited.
- 6.7.2 Users may not leave an open file or session unattended or unsupervised.
- 6.7.3 Users will be held accountable for all activity that occurs under their password and/or account code.
- 6.7.4 Seeking information on, obtaining copies of or modifying files, other data, passwords or account codes belonging to another person is prohibited.
- 6.7.5 Misrepresenting self or other users could be considered fraud and is prohibited.
- 6.7.6 Attempting to gain unauthorized access to the system and/or network is against the law and is prohibited.
- 6.7.7 Communications may not be encrypted so as to avoid security review.
- 6.7.8 Passwords should be changed regularly by the individual using it. Avoid easily guessed passwords.
- 6.7.9 Distributing or otherwise making an employee's password and/or account codes or another person's available to others or otherwise attempting to evade, disable or crack passwords and/or account coded or other security provisions or assisting others in doing so is a serious violation of Saginaw County policies, grounds for immediate suspension of network privileges and other disciplinary action.

## 6.8 Personal Security

- 6.8.1 Personal information such as addresses and telephone numbers should remain confidential when communicating on the network. This includes the user's own as well as those of colleagues and clients where appropriate.
- 6.8.2 Divulging or in any other way making a fellow employee's personal information (including but not limited to, home telephone number(s) and/or address) is prohibited.

## 6.9 Legal

- 6.9.1 The unauthorized installation, use storage or distribution of copyrighted software or material is against the law and is prohibited.
- 6.9.2 Copying of files, passwords or access codes belonging to others will be considered a violation of law, as well as, Saginaw County policies and constitute fraud, plagiarism and/or theft.
- 6.9.3 Software licensed by and to Saginaw County may only be used in accordance with the applicable license.
- 6.9.4 Modifying or damaging information without authorization (including but not limited to altering data, introducing viruses or worms or simply damaging files) is unethical, a violation of Saginaw County policies and may be a felony in Michigan.
- 6.9.5 Using identifiers of other employees, including using such identifiers as one's own, constitutes fraud and is a violation of Saginaw County policies.

## 6.10 Network

- 6.10.1 No use of the network will serve to knowingly or unknowingly disrupt the operation of the network for use by others.
- 6.10.2 System and network components including hardware and software will not be destroyed, modified, abused or tampered with in any way.
- 6.10.3 Users are responsible for the appropriateness and content of material they transmit or publish on the network. Hate mail, harassment, discriminatory remarks or other antisocial behavior such as targeting another person or organization to cause distress, embarrassment, injury, unwanted attention or other substantial discomfort is prohibited. Personal attacks or other action to threaten or intimidate or embarrass an individual, group or organization or attacks based on a person's race, national origin, ethnicity,

disability, religion, gender, veteran status, sexual orientation or another such characteristic or affiliation are prohibited.

6.10.4 Saginaw County, the various departments and ITSC reserve the right to prioritize use of and access to the network.

6.10.5 Saginaw County and ITSC reserve the right to monitor all traffic on the network to maintain network integrity and to ensure that illegal or improper activity is not occurring.

## 6.11 Electronic Mail

6.11.1 Email may not be used for commercial solicitation and/or personal activities.

6.11.2 All county business is to be conducted through county email. Use of personal email for business use is prohibited.

6.11.3 Users must include their email address in all mail sent.

6.11.4 Users must be aware the Internet is not secure and assume that others can read and possibly alter email.

6.11.5 No form of a chain letter or similar communication may be sent on the Internet.

6.11.6 Sending mail that appears to have come from someone else is prohibited.

6.11.7 Minimize large attached files when sending and/or receiving email.

6.11.8 Use extreme caution when receiving emails either internal or external. Verify the legitimacy by reaching out to the sender via phone call before viewing images or downloading attached files and/or programs from persons known or unknown since they may contain malware, ransomware or some other form of malicious entity.

6.11.9 Saginaw County and ITSC consider email to be private. No employee may read or otherwise disclose the contents of any other employee's email unless deemed necessary through the course of an investigation.

6.11.10 Email received at Saginaw County is retained on the system until deleted by the recipient. In addition, because of system backups, unless email is deleted by the recipient it will continue to exist in an offline backup archive file.

6.11.11 Saginaw County and ITSC will not intentionally inspect the contents of email or disclose such contents to other than the sender or intended recipient, without the consent of the sender or intended recipient, unless required by to do so by local, state or federal law or by policies of Saginaw County or to investigate complaints regarding email which is alleged to contain defamatory, inaccurate, abusive, obscene, profane, hateful, sexually oriented, threatening, racially offensive or otherwise illegal material. Saginaw County and ITSC reserve the right to fully cooperate with local, state and/or federal officials in any investigation concerning or relating to any email transmitted from or received at any Saginaw County facility.

## 6.12 System Resources

6.12.1 Diligent effort must be made to conserve system resources. Unused files should be deleted in a timely manner.

6.12.2 Users will accept limitations or restrictions on system and network resources such as but not limited to storage space, time limits or amount of resources consumed when so instructed by ITSC.

6.12.3 Saginaw County and ITSC reserve the right to monitor system and network resources in any form to maintain system and network resources and to ensure that illegal or improper activity is not occurring.

## 6.13 Use Agreement

6.13.1 All employees who desire to have access to the Internet or email must acknowledge they have read, understand, agree and have signed the Acceptable Use Agreement.

6.13.2 All new employees who desire to have access to the Internet or email must complete mandatory training upon assignment thereof by ITSC.

6.13.3 All employees who desire to have access to the Internet or email must complete yearly mandatory cyber security training as assigned by ITSC.

6.13.4 Access will be granted by ITSC on a space available basis, based on the needs of the County and the job description expected of the employee.

6.13.5 ITSC reserves the right to terminate this privilege at any time for violation of these rules and procedures, for higher priority users who need access, for nonuse or other justified causes.

7. ADMINISTRATIVE PROCEDURES: The Information Technology Department shall be responsible for developing and implementing administrative terms or procedures for this policy.

8. CONTROLLER/CAO LEGAL COUNSEL REVIEW: The Controller/CAO has determined that this policy as submitted to the Board of Commissioners contains the necessary substance in order to carry out the purpose of the policy. County Civil Counsel has determined that this policy as submitted contains content that appears to be legal activities of the Saginaw County Board of Commissioners.

Approved as to Substance:  
Saginaw County Controller/CAO

Approved as to Legal Content:  
Saginaw County Civil Counsel

APPROVED: November 23, 1999

AMENDED: June 20, 2023