



MINUTES
Committee on Personnel
Tuesday, January 29, 2013
8:15 a.m.

Tenth Floor Conference Room – Lansing City Hall

CALL TO ORDER

The meeting called to order at 8:15 a.m.

ROLL CALL

Councilmember A'Lynne Robinson, Chair
Councilmember Carol Wood, Vice Chair
Councilmember Brian Jeffries, Member
Councilmember Jody Washington, Member – arrived at 8:20 am

OTHERS PRESENT

Diana Bitely, Council Staff
Arnie Yerxa, Internal Audit
Don Kulhanek, Law

APPROVAL OF MINUTES

None submitted.

PUBLIC COMMENT ON AGENDA ITEMS

None.

DISCUSSION/ACTION

Policies and Procedures

Councilmember Robinson reviewed the changes to "Technology Usage, Computer, Phone, Laptops, I Pads. This also included an addendum to include sanctions for what Council "shall" do in regard to misuse as well as Section 2.101 in the Charter dealing with Public Trust. Questions that had been directed to the Human Resources and IT were reflected in the email and at the present time they unable to provide a list of computer usage violations and consequences for those who have misused city property.

Council President Wood commented on the discipline aspect and the City Attorney's thought that Council is unable to discipline one another. Mason's Manual - 561 Powers of Legislature to Discipline Members" allows for disciplinary actions. "Section 561.1. A legislative body has the right to regular the conduct of its members and may discipline a member as it deems appropriate, including reprimand, censure or expulsion." She questioned if we need a new policy or can Council be included under the definition of "employees".

Councilmember Robinson questioned based upon this finding, why cannot Council Members be disciplined.

Mr. Kulhanek stated that Mason's was not designed for municipal entities. You will find that most constitutions say that the legislative body is responsible for its conduct. This is not covered within the City Charter.

Councilmember Wood disagreed and read a portion that does pertain to the governance of legislators.

Mr. Kulhanek stated that it only provides for punishments if the qualifications are not met within the charter, such as being a resident, a felony, or owing money to the city. He does not see in any legal way where Councilmembers can discipline its members.

Councilmember Jeffries questioned if the computer usage policy does not apply to Council.

Mr. Kulhanek stated that he is still researching how it could apply to Councilmembers because he is not sure how it applies to anyone other than city employees. His hesitance is with regard to Councilmembers having the ability to discipline one another.

Councilmember Wood quoted the definition of "Officer" from the City Charter. "OFFICER includes, but is not limited to, the elected officials of the City, the members of boards and commissions, and their executive staffs, all heads of departments and divisions."

Councilmember Robinson questioned the desire of the Committee in moving forward with the policy. She spoke on the public trust aspect with the offending

Councilmember and the fact that the public is not aware of what is going on and cannot make an educated vote without the information that is relevant.

Councilmember Jeffries questioned why Council cannot speak of the issue that brought this up; the offending Councilmembers.

Mr. Kulhanek stated that there is the potential for litigation.

Councilmember Robinson reiterated that the point is to put something in place to help protect Councilmembers and employees. She feels that Council's hands are tied with regard to this issue. She feels it is unnecessarily complicated and it should be easier. Clearly we want to address the issue at hand, but what is the desire of the Committee?

Councilmember Washington stated that she would like a policy in place that spells out clearly what Councilmembers and staff can and cannot do with the technology made available to them at the expense of the city. She would also like to see a method of sanctions that makes sense.

Councilmember Jeffries stated his confusion that this policy does not apply to Council. It was created with the intent that it would apply to staff and Council and that the Council President would act as the "Department Head". From what he is hearing, there is a possibility that Council is not bound by this policy. Perhaps at the very least, he would like to have a charter amendment prepared that would be broad enough to allow Council to create rules for itself to deal with issues of conduct.

The federal legislation allows a governing body to govern itself with regard to disciplinary actions.

Mr. Kulhanek indicated that he could look into this and potentially draft something.

Councilmember Jeffries commented that the charter only allows for "nothing less than forfeiture".

Mr. Kulhanek stated that Council is covered but there are no consequences for violating it for Councilmembers.

Councilmember Wood questioned in terms of sanctions, what would prevent Council from passing a resolution that states what the offenses were and that would make it public.

Councilmember Jeffries suggested that "the be it further would be to suggest a charter provision."

Councilmember Washington commented that if the IT Department cleaned up the computer, fixed it and gave it back to the Councilmember, that she feels that would be grossly out of line and tampering with a computer that was misused and that if they ignored Council's request to secure the computer and keep it in the condition that it was turned in as.

Councilmember Jeffries requested that Mr. Kulhanek obtain a report outlining where the computer is, what was done to the computer, the hard drive.

Councilmember Robinson stated that this has compromised any potential investigation that could have taken place.

Councilmember Jeffries questioned if Council can require that all laptops be housed at the Council Office.

Councilmember Robinson feels that we are spinning our wheels in terms of this issue.

Mr. Kulhanek stated that he needs additional time to review the changes in policy. This is a new issue for which he has not had time to review it.

Councilmember Wood stated that the original thought was to go paperless and that is why the laptops were purchased; not for personal use during a meeting.

Councilmember Washington stated that we are going to make mistakes, we are human.

Mr. Kulhanek stated that social media policies are not in the policy.

Councilmember Jeffries commented that we feel the policy applies but there is no disciplinary action covered.

Mr. Kulhanek agreed at least at a cursory level.

Councilmember Jeffries questioned if a charter amendment can be done to adopt a way of dealing with these issues. Under the subpoena power, if we are not getting a response from IT, can this Committee subpoena IT for these records.

Mr. Kulhanek stated that the Council body can pass a resolution to issue a subpoena.

Councilmember Robinson commented that we need to adjust the policy that we currently have and get to a resolution that includes a charter amendment. What is the next step if for some reason, this plan is deemed not enforceable by the City Attorney.

Mr. Kulhanek questioned if the housing of the computer at the office would resolve a large part of the issue.

Councilmember Robinson stated that for her it would clear up some of the temptations, such as using the city owned property for personal or commercial business, or for any personal use, or allowing family to utilize the equipment.

The Committee suggested that there be a sign-out process for taking laptops off of the premises.

Councilmember Jeffries requested a written report from IT. If we are unable to obtain that written report, then how does this body subpoena for it.

There was decision about Internal Auditor attending Committee of the Whole meetings and Council meeting, as well to look at the sitting and repairs to the dais.

RECEIPT OF COMMUNICATIONS

None

OTHER

None

PENDING

Computer Usage Policy

ADJOURN

The meeting was adjourned at 9:21 a.m.

Submitted by,

Diana Bitely, Recording Secretary

Lansing City Council

Approved by the Committee on 2/26/2013.

Appropriate documents attached to original set of minutes.



MINUTES
Committee on Personnel
Tuesday, January 29, 2013
8:15 a.m.

Tenth Floor Conference Room – Lansing City Hall

CALL TO ORDER

The meeting called to order at 8:15 a.m.

ROLL CALL

Councilmember A'Lynne Robinson, Chair
Councilmember Carol Wood, Vice Chair
Councilmember Brian Jeffries, Member
Councilmember Jody Washington, Member – arrived at 8:20 am

OTHERS PRESENT

Diana Bitely, Council Staff
Arnie Yerxa, Internal Audit
Don Kulhanek, Law

APPROVAL OF MINUTES

None submitted.

PUBLIC COMMENT ON AGENDA ITEMS

None.

DISCUSSION/ACTION

Policies and Procedures

Councilmember Robinson reviewed the changes to “Technology Usage, Computer, Phone, Laptops, I Pads. This also included an addendum to include sanctions for what Council “shall” do in regard to misuse as well as Section 2.101 in the Charter dealing with Public Trust. Questions that had been directed to the Human Resources and IT were reflected in the email and at the present time they unable to provide a list of computer usage violations and consequences for those who have misused city property.

Council President Wood commented on the discipline aspect and the City Attorney’s thought that Council is unable to discipline one another. Mason’s Manual - 561 Powers of Legislature to Discipline Members” allows for disciplinary actions. “Section 561.1. A legislative body has the right to regular the conduct of its members and may discipline a member as it deems appropriate, including reprimand, censure or expulsion.” She questioned if we need a new policy or can Council be included under the definition of “employees”.

Councilmember Robinson questioned based upon this finding, why cannot Council Members be disciplined.

Mr. Kulhanek stated that Mason’s was not designed for municipal entities. You will find that most constitutions say that the legislative body is responsible for its conduct. This is not covered within the City Charter.

Councilmember Wood disagreed and read a portion that does pertain to the governance of legislators.

Mr. Kulhanek stated that it only provides for punishments if the qualifications are not met within the charter, such as being a resident, a felony, or owing money to the city. He does not see in any legal way where Councilmembers can discipline its members.

Councilmember Jeffries questioned if the computer usage policy does not apply to Council.

Mr. Kulhanek stated that he is still researching how it could apply to Councilmembers because he is not sure how it applies to anyone other than city employees. His hesitance is with regard to Councilmembers having the ability to discipline one another.

Councilmember Wood quoted the definition of “Officer” from the City Charter. “OFFICER includes, but is not limited to, the elected officials of the City, the members of boards and commissions, and their executive staffs, all heads of departments and divisions.”

Councilmember Robinson questioned the desire of the Committee in moving forward with the policy. She spoke on the public trust aspect with the offending

Councilmember and the fact that the public is not aware of what is going on and cannot make an educated vote without the information that is relevant.

Councilmember Jeffries questioned why Council cannot speak of the issue that brought this up; the offending Councilmembers.

Mr. Kulhanek stated that there is the potential for litigation.

Councilmember Robinson reiterated that the point is to put something in place to help protect Councilmembers and employees. She feels that Council's hands are tied with regard to this issue. She feels it is unnecessarily complicated and it should be easier. Clearly we want to address the issue at hand, but what is the desire of the Committee?

Councilmember Washington stated that she would like a policy in place that spells out clearly what Councilmembers and staff can and cannot do with the technology made available to them at the expense of the city. She would also like to see a method of sanctions that makes sense.

Councilmember Jeffries stated his confusion that this policy does not apply to Council. It was created with the intent that it would apply to staff and Council and that the Council President would act as the "Department Head". From what he is hearing, there is a possibility that Council is not bound by this policy. Perhaps at the very least, he would like to have a charter amendment prepared that would be broad enough to allow Council to create rules for itself to deal with issues of conduct.

The federal legislation allows a governing body to govern itself with regard to disciplinary actions.

Mr. Kulhanek indicated that he could look into this and potentially draft something.

Councilmember Jeffries commented that the charter only allows for "nothing less than forfeiture".

Mr. Kulhanek stated that Council is covered but there are no consequences for violating it for Councilmembers.

Councilmember Wood questioned in terms of sanctions, what would prevent Council from passing a resolution that states what the offenses were and that would make it public.

Councilmember Jeffries suggested that "the be it further would be to suggest a charter provision."

Councilmember Washington commented that the IT Department cleaned up the computer, fixed it and gave it back to the Councilmember. She feels that there was a grossly out of line in tampering with a computer that was misused and that they ignored Council's request to secure the computer and keep it in the condition that it was turned in as.

Councilmember Jeffries requested that Mr. Kulhanek obtain a report outlining where the computer is, what was done to the computer, the hard drive.

Councilmember Robinson stated that this has compromised any potential investigation that could have taken place.

Councilmember Jeffries questioned if Council can require that all laptops be housed at the Council Office.

Councilmember Robinson feels that we are spinning our wheels in terms of this issue.

Mr. Kulhanek stated that he needs additional time to review the changes in policy. This is a new issue for which he has not had time to review it.

Councilmember Wood stated that the original thought was to go paperless and that is why the laptops were purchased; not for personal use during a meeting.

Councilmember Washington stated that we are going to make mistakes, we are human.

Mr. Kulhanek stated that social media policies are not in the policy.

Councilmember Jeffries commented that we feel the policy applies but there is no disciplinary action covered.

Mr. Kulhanek agreed at least at a cursory level.

Councilmember Jeffries questioned if a charter amendment can be done to adopt a way of dealing with these issues. Under the subpoena power, if we are not getting a response from IT, can this Committee subpoena IT for these records.

Mr. Kulhanek stated that the Council body can pass a resolution to issue a subpoena.

Councilmember Robinson commented that we need to adjust the policy that we currently have and get to a resolution that includes a charter amendment. What is the next step if for some reason, this plan is deemed not enforceable by the City Attorney.

Mr. Kulhanek questioned if the housing of the computer at the office would resolve a large part of the issue.

Councilmember Robinson stated that for her it would clear up some of the temptations, such as using the city owned property for personal or commercial business, or for any personal use, or allowing family to utilize the equipment.

The Committee suggested that there be a sign-out process for taking laptops off of the premises.

Councilmember Jeffries requested a written report from IT. If we are unable to obtain that written report, then how does this body subpoena for it.

There was decision about Internal Auditor attending Committee of the Whole meetings and Council meeting, as well to look at the sitting and repairs to the dais.

RECEIPT OF COMMUNICATIONS

None

OTHER

None

PENDING

Computer Usage Policy

ADJOURN

The meeting was adjourned at 9:21 a.m.

Submitted by,

Diana Bitely, Recording Secretary

Lansing City Council

Approved by the Committee on 2/4/13.

Appropriate documents attached to original set of minutes.



AGENDA
Committee on Personnel
Tuesday, January 29, 2013 @ 8:15 a.m.
10th Floor Conference Room, City Hall

Councilmember A'Lynne Boles Robinson, Chair
Councilmember Carol Wood, Vice Chair
Councilmember Brian Jeffries, Member
Jody Washington, Member

- 1. Call to Order**
- 2. Roll Call**
- 3. Approval of Minutes**
- 4. Public Comment on Agenda Items**
- 5. Discussion/Action:**
 - A.) Policies and Procedures
- 6. Other**
- 7. Adjourn**
- 8. Pending**



Virg Bernero, Mayor

City of Lansing Computer Usage Policy

I. INTRODUCTION

The City of Lansing maintains its computer system and network for official purposes only. This computer hardware, software and data protection policy reflects the position of the City of Lansing regarding the use of hardware, software and data in all city offices and departments.

Scope

This policy applies to officers and employees working for the City of Lansing on a permanent or temporary basis. It refers to all information resources owned or under control of the City, whether individually controlled or shared. Information resources include any information in electronic or audio-visual format, or any hardware or software that makes possible the storage and use of information. Included in this definition are electronic mail, local databases, externally-accessed databases, all city controlled web sites, CD-ROM, digitized video and photographs and all other digitized information.

II. DATA PROTECTION POLICY STATEMENT

The City of Lansing depends heavily on computer use and information to conduct its business. It is essential that this information be accurate and protected from unauthorized destruction, modification or disclosure.

When using City computers, employees and officers must adhere to the same code of ethics and personnel policies that govern all other aspects of City government. Any actions performed or initiated through the City computer system must be done with integrity, honesty, and compliance with the City's rule of conduct.

The following rules for computer and data use are intended to supplement existing personnel policies by clarifying the expected conduct on employees when working with computers and computer data. If you have a question concerning any computer policy or its applications, consult your department head or the Department of Human Resources.

III. AUTHORIZED USE

Computing resources are provided by the City to accomplish tasks related to the City's mission. These include correspondence, record keeping, administrative support activities, database access and maintenance and other uses specified by an employee's supervisor or job description.

IV. RESTRICTIONS

Issued: 08/01/1998

Reissued: 08/01/2003

Revised: 01/01/2008

All employees must use City computer resources solely for purposes for which they have been authorized. Computing resources may be connected to the Internet or a department or City network for the performance of authorized tasks. Accessing or attempting to access computer resources, the Internet or network to perform unauthorized tasks is not permitted. Employees shall only access data stored or entered in the City's computer systems from their assigned work site during their scheduled work hours and for an authorized purpose. This provision shall not apply to elected officials or Executive Management Plan employees.

Using a computer to access the accounts and files of others or to alter the work product of others without permission is prohibited.

Attempting to subvert network security, impair functionality of the network, or bypass restrictions set by administrators is prohibited. Assisting others in violating these rules by sharing information or passwords is also prohibited.

The improper use or distribution of city owned data or information is prohibited.

The unauthorized use of computer resources, as well as providing false or misleading information for obtaining access to computing facilities, is prohibited. Employees shall not gain unauthorized access to City computing facilities or use City computer resources to gain unauthorized access to other institutions, organizations, or individual computers.

An employee may not authorize anyone to use his/her computer or access his/her database for any reason unless instructed to do so by his/her department head or supervisor. Employees must take all reasonable precautions, such as password maintenance and file protection measures, to prevent the use of his/her computer by unauthorized persons. Employees must not, for example, share a password or dial-in access number with any unauthorized person.

Any use of external networks connected to a department's network or the city's network must comply with the policies of acceptable use promulgated by the Mayor, the employee's department head and this policy statement.

City computer resources may not be used for non-work purposes, commercial activities, financial gain, or entertainment. However, games, entertainment or other programs may be used for education or training purposes if authorized by the department head or supervisor.

All employees who have been authorized to use City computing resources shall regard all personal or proprietary information, which may thereby become available to him/her as confidential. Written permission must be obtained from the appropriate person or body before copying, modifying or otherwise using any part of the information.

Employees shall not copy system files or attempt to access or modify such files or software or computer management programs and data except when authorized to do so by the employee's supervisor or department head.

Employees shall not attempt to modify or repair any computer equipment belonging to or under the control of the City unless authorized to do so by his/her department head or supervisor.

No. 16

City computer equipment shall remain on City premises at all times, with the exception of laptop computers assigned for field use and other exceptions authorized by an employee's department head or supervisor.

No officer or employee shall install or use any encryption program unless specifically told to do so by his/her department head.

Employees shall only access data stored or entered in the City's computer systems from their assigned work site during their scheduled working hours and for an authorized purpose. This provision shall not apply to executive plan employees, non-bargaining unit employees designated by department heads, elected officials, City Council staff or Mayoral staff.

V. SPECIFIC POLICY ELEMENTS

A. Physical Protection of Information and Equipment

All computer equipment is to be secured as best as possible when not in use or left unattended. Laptop computers shall not be left in unlocked vehicles.

Employees who will be out of the office for more than three (3) consecutive workdays shall give his/her assigned laptop computer to authorized personnel for secure storage. (Time out of the office includes, but is not limited to: vacation, sick leave, bereavement, compensation time and conferences.)

All non-server computers shall be logged off upon completion of use or at the end of the work shift.

The security of non-assigned computers shall be protected by logging off at the end of the work shift.

B. Deleting Data or Information

All information or data that is removed from the computer shall be approved by the department head or supervisor. No information shall be permanently deleted from the system without prior authorization. Individual departments may authorize the routine deletion of specific categories of information. Backup and archiving procedures for the retention of deleted data may be established by individual departments.

C. Remote Access Policy

Remote access to city computers by officers, employees and vendors shall be by prior approval of the department head.

D. Email

Email is to be used for conducting City business. Email is not to be used as a form of entertainment or as a forum for political, religious or any other personal expression inconsistent with work place responsibilities.

Issued: 08/01/1998
Reissued: 08/01/2003
Revised: 01/01/2008

The email system and its contents are the property of the City of Lansing and employees have no expectation of privacy in its use or content. For example, a single email sent to just one person can be forwarded, without the permission of the sender, to hundreds of others either intentionally or inadvertently. Employees should also be aware that deleted messages are not always deleted completely. They may appear on backup tapes, on other computers or in other employee's email boxes. In addition, email exchanges are subject to release under the Freedom of Information Act.

Even though there is no expectation of privacy in City email, no City employee is to use his or her position or access rights to read another employee's email or personal files. The only people authorized to do this are individual department heads. The Director of Management Services may also, in consultation with affected department head(s), direct authorized persons to access individual email accounts.

E. Privacy Rights and Limitations

No privacy rights exist to any personal files or email created or received on city computer resources. As stated previously, City computer equipment is to be used to conduct City business and therefore any personal information stored or created on this equipment is subject to review and elimination by appropriate authorities.

The City of Lansing is a government unit and is therefore subject to the Freedom of Information Act (FOIA). As such, electronic information and email created in the performance of employee job duties may be considered a public record. Therefore, all computer files generated by city officers and employees are subject to review and possible release. Even personal email or files not related to the specific issue discussed in the FOIA request may be examined in the course of responding to a FOIA request.

System administrators or other city personnel may also need to gather information from computers to ensure the continued functioning of computer resources or to investigate complaints. This may require the examination of activity logs, files, email, and printer listings to gather information necessary to diagnose and correct problems with system software or hardware. Individual computer files may also be examined to determine if policy violations have occurred or are occurring.

Privacy policies contained in other city documents should also be followed when working with computer data.

F. Password

The purpose of passwords is to protect the City's database and information from corruption or use by unauthorized individuals. The issuance of a password to an employee is not consent to develop or protect personal files.

All passwords are considered confidential information and may not be disclosed. A password may not be used by anyone other than the person(s) who has been authorized to use it.

All employees must notify their department head or supervisor if they believe their password is being used or has been compromised by others.

G. Virus Protection

City computers should be protected by software that scans for viruses. Virus detection helps avoid destruction of computer files and hard drives. However, since virus protection software is not 100% effective, it is extremely important to follow procedures to protect computer data. This is an important issue and if a damaging virus were to destroy a hard drive's contents, the cost to the City of Lansing could be thousands of dollars.

The following steps shall be followed when using software on City computers:

- The installation and use of software not owned by the City is prohibited without authorization from the department head or supervisor.
- Virus scanning programs shall not be disabled.
- Employees who are authorized to transfer data from demo disks or disks brought from home must follow the virus scanning and installation procedures established by their department.
- Any software downloaded from an outside source shall not be loaded without approval from the department head or supervisor.

H. Network Security

Network security is dependent on employees. Each employee or group of employees has a set of specific rights on individual computers and file servers. Each Department may establish employee privileges based on an employee's job function. Specific user groups and access privileges may be defined by the department head, supervisor, or system administrator. These access privileges determine which files or data an employee may access.

I. Software Use

In cases where software is copyrighted or otherwise protected, employees may not copy or distribute the software unless authorized to make a back-up copy. Furthermore, it is illegal to facilitate access by others to copyrighted software.

It is the responsibility of each department that maintains a computer system to insure that all software on that system is appropriately licensed. It is the responsibility of the data processing department to insure that the software it installs is appropriately licensed.

The City forbids, under any circumstances, the unauthorized reproduction of software or use of illegally obtained software. Using City equipment to make illegal copies of software is prohibited. City employees who violate this policy are subject to disciplinary action and/or legal action by the City. Individuals who violate U.S. copyright law and software licensing agreements may also be subject to criminal or civil legal action.

City employees are required to follow conditions or restrictions required by the licensing agreements for software programs purchased by the departments. For commonly used applications, the following conditions apply:

Issued: 08/01/1998
Reissued: 08/01/2003
Revised: 01/01/2008

- It is illegal to copy a software program, such as WordPerfect, Lotus 1-2-3, Norton Utilities, and install that single program for simultaneous use on multiple machines. (Note: some software applications allow installation on a home computer as well as a work computer.)
- Unauthorized copies of software programs may not be used on City equipment. This applies even though you may not have made the illegal copy.
- The purchase of the appropriate number of copies of a software program is necessary for maintaining legal status, especially if you are using machines connected to a network.
- City employees are prohibited from assisting in making or using illegal copies of City-owned software.
- City employees are permitted to make an archival (back-up) copy of a software program.

J. Internet Use

Internet access from City computers is to be used for City business. Individual departments may authorize and define business use.

No program or application shall be downloaded from the Internet and installed on City computers without prior permission of the department head or supervisor.

VI. VIOLATIONS

The following list of policy violations is not all inclusive but merely illustrative:

- Knowingly accessing or attempting to access any computer system, data or information which an employee does not have permission or authority to access is a violation of this policy.
- Using, copying, modifying or transferring data that is not part of an employee's assigned responsibilities is a violation of this policy.
- Using computer hardware, data or information on City computers for personal or financial gain is a violation of this policy.
- Accessing a computer or network for the purpose of altering, damaging or destroying software, data or information, regardless of its location, is a violation of this policy.
- Giving access codes or passwords to any individual not authorized to receive them is a violation of this policy.

VII. RESPONSIBILITIES AND CONSEQUENCES OF NON-COMPLIANCE

All officers, employees and temporary workers employed by the City are expected to comply with this policy. Any employee who violates this policy is subject to disciplinary action

Issued: 08/01/1998
Reissued: 08/01/2003
Revised: 01/01/2008

consistent with personnel policies and may be subject to criminal or civil prosecution under applicable laws.

Any officer or employee who has reason to believe that a coworker may be misusing City computer resources or violating any aspect of this policy shall voice his or her concern to his or her department head or supervisor. Department heads and supervisors are responsible for addressing any policy violations of which they become aware. Department heads may refer the matter to the Department of Human Resources if appropriate.

VIII. POLICY MODIFICATIONS OR CHANGES

Individual departments may make additions to this policy and exercise discretionary authority where indicated as long as the additional policies do not contradict or nullify this policy or other established personnel policies.

CITY OF EAST LANSING

TECHNOLOGY AND COMPUTER USE POLICY

1.0 OVERVIEW

The department of Information Systems intention for publishing an Acceptable Use Policy is not to impose restrictions that are contrary to the City of East Lansing's established culture of openness, trust and integrity. The department of Information Systems is committed to protecting the City of East Lansing's employees, partners and the city from illegal or damaging actions by individuals, either knowingly or unknowingly.

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail and web browsing are the property of the City of East Lansing. These systems are to be used for business purposes in serving the interests of the city, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details.

The I.S. department maintains the Computer and Technology Resource Usage Policy on behalf of the City of East Lansing. However, other departments may develop supplemental policies and controls to accommodate specific requirement so long as these policies do not compromise the city's policies and controls. This policy is also subject to IT General Controls as required by law and by audit such as compliance audits by vendors or third-party institutions retained for such purposes.

Effective security is a team effort involving the participation and support of every City of East Lansing employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 PURPOSE

The purpose of this policy is to outline the acceptable use of computer equipment at the City of East Lansing. These rules are in place to protect the employee and the City of East Lansing. Inappropriate use exposes the City of East Lansing to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 SCOPE

This policy applies to employees, contractors, consultants, temporaries, and other workers at the City of East Lansing, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by the City of East Lansing.

4.0 POLICY

4.1 General Use and Ownership

1. While the City of East Lansing's network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of the City of East Lansing. Because of the need to protect the City of East Lansing's network, management cannot guarantee the confidentiality of information stored on any network or local device belonging to the City of East Lansing.
2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.



CITY OF EAST LANSING

3. For security and network maintenance purposes, authorized individuals within the City of East Lansing may monitor equipment, systems and network traffic at any time.
4. The City of East Lansing reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Access to computer rooms will be limited to staff who require access for the normal performance of their jobs. Computers with sensitive information installed on the local disk drive should be secured in a locked room or office during non-business hours. Equipment which is to be removed from City of East Lansing property must be approved in advance with the I.S. department and an inventory of this equipment maintained by I.S.
2. Only legally licensed software will be installed on City of East Lansing computers. Users are expected to read, understand and conform to the license requirements of any software product(s) they use or install. Software cannot be copied or installed without the permission or involvement of the I.S. department.
3. I.S. will configure all workstations with virus protection software, which should not be removed or disabled. Each employee is responsible for protecting their computer against virus attack by following I.S. guidelines for scanning all incoming communications and media, and by not disabling the anti-virus application installed on their workstation. All data disks and files entering or leaving City of East Lansing should be scanned for viruses.
4. All staff will log out of the network and turn their computers off before leaving the office at night. Staff should log off of the network when they will be away from their desk for an extended period.
5. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.
6. Because information contained on portable computers is especially vulnerable, special care should be exercised when using, storing, or transporting portable (laptop) computers.
7. Postings by employees from the City of East Lansing email address to newsgroups should not occur unless posting is in the course of business duties.
8. All hosts used by the employee that are connected to the City of East Lansing Internet/Intranet/Extranet, whether owned by the employee or the City of East Lansing, shall be continually executing approved virus-scanning software with a current virus database unless overridden by departmental or group policy.
9. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the City of East Lansing authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing the City of East Lansing owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Employees are expected to use the standard software provided by I.S., or identify applications they need in the course of their work. Staff members are not permitted to download applications, demos



CITY OF EAST LANSING

or upgrades without the involvement of I.S.. Employees will use the standard e-mail system provided by City of East Lansing for official e-mail communications, and should not install their own e-mail systems. Additionally, use of instant messaging programs, such as ICQ, AOL Instant Messenger, Microsoft Messenger, etc., is prohibited unless otherwise approved by management or the I.S. department.

2. Any and all information, statistics, and other information system data including email, internet logs, computer files, and so on are property of the City of East Lansing and are subject to monitoring by the City. In addition, employees should be mindful that there is no assurance that e-mail texts and attachments sent within the company and on the Internet will not be seen, accessed or intercepted by unauthorized parties.
3. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the City of East Lansing.
4. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which the City of East Lansing or the end user does not have an active license is strictly prohibited.
5. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
6. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
7. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
8. Using a the City of East Lansing computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
9. Making fraudulent offers of products, items, or services originating from any the City of East Lansing account.
10. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
11. Port scanning or security scanning is expressly prohibited unless prior notification to the Information Systems department is made.
12. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
13. Circumventing user authentication or security of any host, network or account.
14. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
15. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
16. Providing information about, or lists of, the City of East Lansing employees to parties outside the City of East Lansing.
17. Using a computer account that you are not authorized to use. Obtaining a password for a computer account without the consent of the account owner.
18. Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks.
19. Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network.



CITY OF EAST LANSING

20. Attempting to circumvent data protection schemes or uncover security loopholes.
21. Deliberately wasting computing resources.
22. Using electronic mail to harass others.
23. Masking the identity of an account or machine.
24. Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within the City of East Lansing's networks or other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by the City of East Lansing or connected via the City of East Lansing's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).
8. The City of East Lansing employees shall have no expectation of privacy in anything they store, send or receive on the company's email system. The City of East Lansing may monitor messages without prior notice. The City of East Lansing is not obliged to monitor email messages.
9. The City of East Lansing email system shall not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, hair color, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin. Employees who receive any emails with this content from any City of East Lansing employee should report the matter to their supervisor immediately.

4.4 Password Security

1. Initial passwords are assigned by the I.S. department and should not be given to other staff or persons outside the organization.
2. Employees should change the provided passwords as soon as possible using the instructions provided by the I.S. staff.
3. The City of East Lansing reserves the right to override any employee-selected passwords and/or codes. Periodically, staff may be required to change their passwords.
4. At no time should a City of East Lansing employee allow a temporary, contractor or another employee use of their login. In the case where an employee does provide another person access to their account, they will be responsible for the actions of the individual using their account.
5. Passwords should not be stored in computer data files, on the network, or be displayed openly at any workstation.

4.5 Blogging

1. Blogging by employees, whether using the City of East Lansing's property and systems or personal computer systems, is also subject to the terms and restrictions set forth in this Policy for acceptable use of the City's information systems.
2. The City of East Lansing's Confidential Information policy also applies to blogging. As such, Employees are prohibited from revealing any City of East Lansing confidential or proprietary



CITY OF EAST LANSING

- information, trade secrets or any other material covered by the City of East Lansing's Confidential Information policy when engaged in blogging.
3. Employees shall not engage in any blogging that may harm or tarnish the image, reputation and/or goodwill of the City of East Lansing and/or any of its employees. Employees are also prohibited from making any discriminatory, disparaging, defamatory or harassing comments when blogging or otherwise engaging in any conduct prohibited by the City of East Lansing's Non-Discrimination and Anti-Harassment policy.
 4. Employees may also not attribute personal statements, opinions or beliefs to the City of East Lansing when engaged in blogging. If an employee is expressing his or her beliefs and/or opinions in blogs, the employee may not, expressly or implicitly, represent themselves as an employee or representative of the City of East Lansing. Employees assume any and all risk associated with blogging.
 5. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, the City of East Lansing's trademarks, logos and any other the City of East Lansing intellectual property may also not be used in connection with any blogging activity

4.6 Internet Usage

1. This policy applies to all uses of the Internet, but does not supersede any state or federal laws or company policies regarding confidentiality, information dissemination, or standards of conduct.
2. The use of city automation systems is for business purposes only. Brief and occasional personal use is acceptable as long as it is not excessive or inappropriate, occurs during personal time (lunch or other breaks), and does not result in expense to the City of East Lansing.
3. The Internet is to be used to further the City of East Lansing's mission, to provide effective service of the highest quality to the city's customers and staff, and to support other direct job-related purposes.
4. All policies and procedures apply to employees' conduct on the Internet, especially, but not exclusively, relating to: intellectual property, confidentiality, city information dissemination, standards of conduct, misuse of city resources, anti-harassment, and information and data security.
5. Use of City of East Lansing computer, network, or Internet resources to access, view, transmit, archive, or distribute racist, sexist, threatening, or otherwise objectionable or illegal material is strictly prohibited. "Material" is defined as any visual, textual, or auditory item, file, page, graphic, or other entity. Such material violates the city's anti-harassment policies and is subject to company disciplinary action.
6. No employee may use the City of East Lansing's Internet/Intranet facilities to deliberately propagate any virus, worm, Trojan horse, trap-door program code, or other code or file designed to disrupt, disable, impair, or otherwise harm either the city's networks or systems or those of any other individual or entity.

5.0 ENFORCEMENT

Any employee found to have violated this policy and/or state and federal laws may be subject to disciplinary action, up to and including termination of employment and possible criminal prosecution.

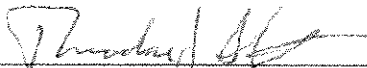
6.0 DEFINITIONS

Term	Definition
<i>Blogging</i>	Writing a blog. A blog (short for weblog) is a personal online journal that is frequently updated and intended for general public consumption.
<i>Spam</i>	Unauthorized and/or unsolicited electronic mass mailings.
<i>Email</i>	The electronic transmission of information through a mail protocol such as SMTP or IMAP. Typical email clients include Eudora and Microsoft Outlook.
<i>Forwarded email</i>	Email resent from an internal network to an outside point



CITY OF EAST LANSING

Chain email or letter	Email sent to successive people. Typically the body of the note has direction to send out multiple copies of the note and promises good luck or money if the direction is followed.
Sensitive information	Information is considered sensitive if it can be damaging to the City of East Lansing.
Virus warning.	Email containing warnings about virus or malware. The overwhelming majority of these emails turn out to be a hoax and contain bogus information usually intent only on frightening or misleading users.
Unauthorized Disclosure	The intentional or unintentional revealing of restricted information to people, both inside and outside the City of East Lansing who do not have a need to know that information.
Excessive Use	Use is defined as "excessive" if it interferes with normal job functions, responsiveness, or the ability to perform daily job activities.
Intranet	An intranet is a private computer network that uses <u>Internet protocols</u> and <u>network</u> connectivity to securely share part of an organization's information or operations with its employees. Sometimes the term refers only to the most visible service, the internal website.
Extranet	An extranet is a private network that uses <u>Internet protocols</u> , <u>network</u> connectivity, and possibly the public telecommunication system to securely share part of an organizations information or operations with suppliers, vendors, partners, customers or other businesses.


Theodore J. Staton, City Manager

8-13-09
Dated



ACCEPTABLE USE AND INTERNET SAFETY POLICY

With the spread of telecommunications throughout society, including the educational environment, the Jackson Public School District Board of Trustees recognizes that students and employees will shift the way they access and transmit information, share ideas, and communicate with others. As schools and offices are connected to the global community, the use of new tools and technologies brings new responsibilities as well as opportunities. Network resources are intended for educational purposes and to carry out the legitimate business of the school district. The Jackson Public School District Board of Trustees expects all users of the district's computing and network resources, including electronic mail and telecommunications tools, to utilize these resources appropriately.

It is the policy of the Jackson Public School District to: (a) prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications; (b) prevent unauthorized access and other unlawful online activity; (c) prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and (d) comply with the Children's Internet Protection Act [Pub. L. No. 106-554 and 47 USC 254(h)].

Education, Supervision and Monitoring

It shall be the responsibility of all members of the Jackson Public School District to educate, supervise and monitor appropriate usage of the online computer network and access to the Internet in accordance with this policy, the Children's Internet Protection Act, the Neighborhood Children's Internet Protection Act, and the Protecting Children in the 21st Century Act.

Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the Information Technology Department.

The Instructional Technology Department will provide age-appropriate training for students who use the District's Internet facilities. The training provided will be designed to promote the District's commitment to:

- a. The standards and acceptable use of Internet services as set forth in the District's Internet Safety Policy;
- b. Student safety with regard to: safety on the Internet; appropriate behavior while online, on social networking Websites, and in chat rooms; and cyberbullying awareness and response.
- c. Compliance with the E-rate requirements of the Children's Internet Protection Act ("CIPA").

Following receipt of this training, the student will acknowledge that he/she received the training, understood it, and will follow the provisions of the District's acceptable use policies.

Access to Inappropriate Material

To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate

information.

Specifically, as required by the Children’s Internet Protection Act, blocking shall be applied to visual depictions of materials deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled for adults or, in the case of minors, minimized only for bona fide research or other lawful purposes.

Section I: DEFINITIONS

A. Child Pornography

The term “child pornography” has the meaning given such term in section 2256 of title 18, United States Code.

B. Harmful to Minors

The term “harmful to minors” is defined by the Communications Act of 1934 (47 USC Section 254 [h][7]), as meaning any picture, image, graphic image file, or other visual depiction that taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

C. Minor

The term “minor” means an individual who has not attained the age of 17.

D. Obscene

The term “obscene” has the meaning given such term in section 1460 of title 18, United States Code.

E. Sexual Act; Sexual Contact

The terms “sexual act” and “sexual contact” have the meanings given such terms in section 2246 of title 18, United States Code.

F. Directory Information

The term “directory information” is defined by FERPA, (20 USC § 1232g; 34 CFR Part 99), as information contained in an education record of a student that would not generally be considered harmful or an invasion of privacy if disclosed. It includes, but is not limited to, the student’s name, address, telephone listing, electronic mail address, photograph, date and place of birth, major field of study, dates of attendance, grade level, enrollment status, participation in officially recognized activities and sports, weight and height of members of athletic teams, degrees, honors and awards received, and the most recent educational agency or institution attended.

Section II: Acceptable Use

A. Acceptable Uses of Network

The Jackson Public School District is providing access to its computer networks and the Internet *only* for educational purposes or to carry out the legitimate business of the school district.

B. Unacceptable Uses of Network

Among the uses that are considered unacceptable and which constitute a violation of this policy are, but are not limited to, the following:

1. Uses that violate the law or encourage others to violate the law
Examples include: transmitting offensive or harassing messages; offering for sale or use any substance the possession or use of which is prohibited by the district's Student Code of Conduct; viewing, transmitting, or downloading pornographic materials or materials that encourage others to violate the law; intruding into the networks or computers of others; and downloading or transmitting confidential, trade secret information, or copyrighted materials
2. Uses that cause harm to others or damage to their property
Examples include: engaging in defamation (harming another's reputation by lies); employing another's password or some other user identifier that misleads message recipients into believing that someone other than you is communicating or otherwise using his/her access to the network or the Internet; uploading a worm, virus, or other harmful form of programming or vandalism; participating in hacking activities or any form of unauthorized access to other computers, networks, or information systems
3. Uses that jeopardize the security of user access and of the computer network or other networks on the Internet.
Examples include: disclosing or sharing your password with others; impersonating another user
4. Uses that are commercial or political in nature
Examples include: using the network for personal financial gain or profit; using the network to give others private information about yourself or others, including credit card numbers and social security numbers
5. Uses that cause harm to the district's computer, network, or equipment
Examples include: installing software programs, instant messaging programs, altering system settings, or otherwise reconfiguring computers without approval of the appropriate personnel
6. Uses that is inconsistent with the purpose of the network and internet.
Examples include: using internet games, chat rooms, and instant messaging not specifically assigned by a teacher or administrator; downloading music or video files or any other files that are not directly related to a school assignment

C. Netiquette

All users must abide by rules of network etiquette, which include the following:

1. Be polite. Use appropriate language. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language.
2. Avoid language and uses that may be offensive to other users. Do not use, make, distribute, or redistribute jokes, stories, or other material, which is based upon slurs or stereotypes relating to race, gender, ethnicity, nationality, religion, or sexual orientation.
3. Do not assume that a sender of e-mail is giving his or her permission for you to forward or redistribute the message to third parties or to give his/her e-mail address to third parties.
4. Be considerate when sending attachments with e-mail (where permitted). Be sure the

file is not too large to be accommodated by the recipient's system and is in a format the recipient can open.

Section III: Internet Safety

A. General Warning

All users, and the parents/guardians of minor users, are advised that access to the electronic network may include the potential for access to materials inappropriate for school-aged pupils. Every user must take responsibility for his/her use of the computer network and internet and stay away from these sites. If a student finds that other users are visiting offensive or harmful sites, he/she should report such use to the person designated by the school.

B. Personal Safety

Be safe. In using the computer network and Internet, do not reveal personal information such as your home address or telephone number. Do not use your real last name or any other information which might allow a person to locate you without first obtaining the permission of a supervising teacher. If you are a minor, do not arrange a face-to-face meeting with someone you "meet" on the computer network or Internet without your parent's permission. Regardless of your age, you should never agree to meet a person you have only communicated with on the Internet in a secluded place or in a private setting.

C. Hacking and Other Illegal Activities

It is a violation of this policy to use the district's computer network or the Internet to gain unauthorized access to other computers or computer systems, or to attempt to gain such unauthorized access. Any use which violates state or federal law relating to copyright, trade secrets, the distribution of obscene or pornographic materials, or which violates any other applicable law or municipal ordinance, is strictly prohibited.

D. Confidentiality of Student Information

Personal identifiable information concerning minor students may not be disclosed or used in any way on the Internet without the permission of a parent or guardian, or for non-minors, without the person's consent. Users should never give out private or confidential information about themselves or others on the Internet, particularly credit card numbers and Social Security numbers.

The schools or district may authorize the release of directory information, as defined by FERPA, for internal administrative purposes, approved educational projects, activities, and publications. As stipulated by FERPA, parents will be offered the opportunity to deny publication of directory information. Parents also will be given the opportunity to deny publication of non-directory information such as student work.

E. Active Restriction Measures

The Jackson Public School District will utilize filtering software or other technologies to attempt to prevent students from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors.

The district will also monitor the online activities of students, through direct observation and/or technological means, to ensure that students are not accessing such depictions or any other material that is inappropriate for minors. Internet access without filters will be offered to employees at specific locations, e.g., Teacher Resource Center, for purposes of bona fide research or other educational projects.

Section IV: E-Mail

All network users assigned an e-mail account signify by their acceptance of the account their willingness to adhere to this policy regarding acceptable use. Failure to adhere to these guidelines may result in the loss of the electronic mail account and access to the Internet and may lead to further disciplinary action up to and including termination. Furthermore, any activity that may be in violation of local, state, or federal laws will be reported to the appropriate law enforcement agency.

Section V: Privacy

Network and Internet access is provided as a tool for education. The Jackson Public School District reserves the right to monitor, inspect, copy, review, and store at any time and without prior notice, any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. All such information files shall be and remain the property of the district, and no user shall have any expectation of privacy regarding such materials.

Section VI: Failure to Follow Policy

The use of the computer network and Internet is a privilege, not a right, and inappropriate use will result in a loss or restriction of network privileges, disciplinary action, and/or referral to legal authorities. The network administrators will close an account when necessary. An administrator or faculty member may request the network administrator to deny, revoke, or suspend specific user access and/or user accounts.

Section VII: Warranties/Indemnification

The Jackson Public School District's website or individual Jackson Public Schools' sites might link, or connect, to another site that might link to a site that contains objectionable material that the school district does not embrace or promote. While the district will attempt to prevent connections that are objectionable, the links are not under the district's control. Therefore, the district will not be responsible for the contents of a linked site. The links are provided only as a convenience and the district does not endorse or imply endorsement of the linked site.

The Jackson Public School District makes no warranties of any kind, either express or implied, in connection with its provision of access to and use of its computer networks and the Internet provided under this policy. It shall not be responsible for any claims, losses, damages, or costs (including attorney's fees) of any kind suffered, directly or indirectly, by any user or his or her parent(s) or guardian(s) arising out of the user's use of its computer networks or the Internet

under this policy. By signing the Jackson Public School District's Acceptable Use and Internet Safety Contract, a user is taking full responsibility for his or her use, and the user who is 18 or older or, in the case of a user under 18, the parent(s) or guardian(s), are agreeing to indemnify and hold the school, the Jackson Public School District, and all of the administrators, teachers, and staff harmless from any and all loss, costs, claims, or damages resulting from the user's access to its computer network and the Internet, including, but not limited to, any fees or charges incurred through purchases of goods or services by the user. The user or, if the user is a minor, the user's parent(s) or guardian(s) agree to cooperate with the district in the event of the district's initiating an investigation of a user's use of his/her access to its computer network and the Internet, whether that Jackson Public Schools' network access is on a district computer or on another computer outside the district's network.

The superintendent or the superintendent's designee has the authority to amend or revise the Acceptable Use and Internet Safety Contract as deemed necessary and appropriate consistent with this policy.

SOURCE: Jackson Public School District, Jackson, Mississippi

LEGAL REF.: Children's Internet Protection Act; Public Law 106-554; Family Educational Rights and Privacy Act (20 USC § 1232g)

DATE: July 17, 2000

AMENDED: August 19, 2002
June 26, 2012

ACCEPTABLE USE AND INTERNET SAFETY CONTRACT

User Name _____ Date _____

School/Location _____ Grade _____

Home Address _____ Home Phone _____

I certify that I have read the district's Acceptable Use and Internet Safety Policy. I understand and agree to follow all of the terms and conditions of the policy. I understand any violation of the district policy will result in the temporary or permanent loss of network and/or Internet access and/or my user account; may result in other disciplinary action; and may constitute a criminal offense. I agree to report any misuse of the Internet resources to the appropriate network administrator. In consideration for the privilege of using the district's computers, network, and Internet access, I hereby release and hold harmless the district and its employees, from any and all claims and damages of any nature arising from my use, or inability to use, the district's computers, network, or Internet access.

User Signature _____

Parent or Guardian Agreement (For students under age 18)

As the parent or legal guardian of the above student, I have read, understand, and agree that my child or ward shall comply with the terms of the Jackson Public School District's Acceptable Use and Internet Safety Policy for the student's access to the Jackson Public School District's computer network and the Internet. I understand that access is being provided to the student for educational purposes only. Although the district will utilize filtering software or other technologies to prevent students from accessing unacceptable content through the network or Internet, I understand that it is impossible for the school to restrict access to all offensive and controversial materials and understand my child's or ward's responsibility for abiding by the policy. I am, therefore, signing this contract and agree to indemnify and hold harmless the school, the Jackson Public School District, the administrators, and teachers against all claims, damages, losses, and costs, of whatever kind, that may result from my child's or ward's use of his or her access to such networks or his or her violation of the district's policy.

I hereby give permission for my child or ward to use the approved account to access the computer network and the Internet.

Parent/Guardian Name _____ Date _____

Address _____ Home Phone _____

Parent or Guardian Signature _____

INGHAM COUNTY

Policy Regarding the Use of County Resources, Including Information Technology Resources

Approved June 12, 2001

Introduction

This policy sets forth Ingham County's policies with regard to the use of county resources generally, and information technology ("IT") resources specifically. County resources generally refer to county equipment and supplies (desks, vehicles, office supplies, copiers, etc) provided by the county to assist employees in carrying out their work. IT resources refer specifically to items such as personal computers, software, the county network, phones, the county provided Internet connection, the county web page and Intranet; e-mail, electronic voice and video communication, facsimile, the Internet and future technologies). The policy addresses, among other things, county access to, review or disclosure of electronic files, electronic mail and electronic voice and video communications through or stored on any part of the county's IT resources. These policies do not constitute a contract. The County reserves the right to change them at any time.

I.

General Policy

County resources generally, and IT resources specifically, may be provided to employees exclusively to assist in the efficient and effective day to day operations of offices, departments and agencies. Their intended use includes the facilitation of the employees work; collaboration and exchange of information within and between County departments, agencies, other employees, other branches of government and the public. Their use also includes providing the public with enhanced access to services and information.

County department heads, elected Officials, and the Chief Judge, with technical assistance from the MIS Department if necessary, have the capability to access, review, copy, modify and delete any information transmitted or stored in IT resources, including voice and e-mail messages. The appropriate County department head, elected Official, or the Chief Judge reserve the right to access, review, copy, modify or delete all such information for any purpose and to disclose it to any party if legally compelled to do so, pursuant to the Freedom of Information Act, or if the County otherwise deems it appropriate. Those voice or other IT resources files containing personal information of an employee as a result of an employee's making incidental use of the IT resources system for personal purposes, including the transmission of personal voice and e-mail messages, will be treated no differently than other files, i.e., the County department heads, elected Officials, and the Chief Judge reserve the right to access, review, copy, modify, delete or disclose them for any purpose required by law, or which the County department heads, elected Officials, and the Chief Judge deem appropriate in its discretion. Accordingly, employees should not use the IT resources system to send, receive or store any personal information that they wish to keep private. Employees should treat the IT resources system like a shared file system -- the files or messages sent, received or stored anywhere in the respective systems will be available for review by the appropriate County department head, elected Official, or the Chief Judge and, may be disclosed to third parties.

Software developed using county equipment or on County time is the property of the county. Access to County resources shall be through a password as made available by the Management Information Systems Department ("MIS Department").

Expectations of appropriate use are set and enforced by the county-wide elected

official, Chief Judge, department head, or as set forth by statute.

II.

Prohibited Uses of County Resources

County resources generally, and IT resources specifically, may be provided to employees exclusively to assist in the efficient and effective day to day operations of offices, departments, and agencies. Notwithstanding the foregoing, the following uses of county resources, including IT resources, are strictly prohibited, and violation of these policies may result in discipline, up to and including immediate discharge and, where appropriate, civil and/or criminal liability. This list is not intended to be all-inclusive and individuals may be disciplined, or subject to civil or criminal liability for matters not listed below:

1. Knowingly or negligently viewing, downloading, or any distribution or solicitation of offensive or harassing statements, transmission of defamatory, obscene, offensive or harassing messages or messages that disclose personal information without authorization.
2. Knowingly or negligently viewing, downloading, or any distribution or solicitation of incendiary statements which may incite violence or describe or promote the use of weapons or devices associated with terrorist activities.
3. Knowingly or negligently viewing, downloading, or any distribution or solicitation of sexually oriented messages or images that are unrelated to the duties being performed.
4. Any use of County-provided resources for illegal purposes or in support of such activities.
5. Any use of county resources for commercial purposes, product advertisement or "for-profit" personal activity unless authorized for this purpose.
6. Any sexually explicit use, whether visual or textual that is unrelated to the duties being performed.
7. Any use for religious or political lobbying.

III.

Prohibited Uses of IT Resources

1. Duplicating, transmitting or using software which is not in compliance with software licensing agreements and/or unauthorized use of copyrighted materials or other person's original writings.
2. Security violations including, but not limited to:
 - A. Accessing accounts or information within or outside the County's computers and communications facilities for which an employee is not authorized or does not have a business need;
 - B. Knowingly or inadvertently spreading computer viruses.
 - C. Transmitting confidential and/or attorney-client privileged communication and information without proper security and authority.
 - D. Misuse of another's password, negligent or intentional disclosure of the assigned password or any attempt to defeat the password security.
3. Modifying or altering software, programs or the standardized configuration of the equipment supplied by the County including software, hardware, and OS system files without prior authorization from the MIS Department.
4. Installing, removing, storing, uploading or downloading software or programs to the IT system without prior

approval from the MIS Department. All approved installations must be performed by MIS personnel or at their direction.

5. Making available a network service (FTP server, WWW server, etc.) without written permission from the MIS Department.

6. Moving county equipment from its MIS designated location to a new location without prior authorization from the MIS Department.

7. Installing hardware or software without permission of MIS.

8. Intentionally wasting IT resources by, for example:

A. Placing a program in an endless loop; or,

B. Disrupting the use or performance of County-authorized IT resources or any other computer system or network

C. Distributing "junk mail" such as chain letters, advertisements or unauthorized solicitations.

9. Making available any access to the County's telecommunications equipment, computers, or associated media without written authorization from the MIS Department.

- Using the computer system to copy and/or transmit software programs, documents or other information protected by copyright law.

Policy Implementation

The Ingham County Board of Commissioners has adopted the County Resources Policy to govern the use of county resources, including IT resources, and reserves the right to change any portion of it at any time.

There are three groups involved with the implementation of the County Resources Policy: 1) the County-wide elected officials, Chief Judges, and Department Heads; 2) the MIS Department; and 3) the Information Systems Advisory Committee.

Except as provided by this policy, the County-wide elected officials, Chief Judges, and Department Heads are responsible for determining and enforcing appropriate use of county resources, including IT resources, by employees or contractors under their supervision and control. County-wide elected officials, Chief Judges, and Department Heads may establish standards of appropriate use which are more stringent than defined in this policy.

Where authorization by the MIS Department is required, the MIS Director is responsible for issuing guidelines for obtaining such authorization. The guidelines may include the delegation of authorization to others, including departmental MIS liaisons or the County-wide elected officials, Chief Judges, or Department Heads.

The Information Systems Advisory Committee ("ISAC") advises and assists the MIS Department in the development of long term county resource plans, implementation of system upgrades and new technologies, development of operational procedures affecting users, and the resolution of conflicts involving county resources. The ISAC is responsible for monitoring the overall effectiveness of the County Resources Policy and for recommending changes to the policy. The ISAC will also review any proposed guidelines implementing the policy which are proposed by the MIS Director, prior to their issuance.

Membership on the ISAC shall be comprised of representatives from the major program areas of the County: two representatives from the area of Law and Courts, one from the Human Services area, one from the Administrative Services area, and the Board Coordinator. Representatives shall be appointed by the Controller in consultation with the MIS Director.

Ingham County Resource Use Policy

Ingham County employees, County-wide elected official, Judges and Department Heads are encouraged to use the ISAC to proactively address issues relating to the enhancement of technology within Ingham County government.

1460.00 Acceptable Use of State of Michigan Department of Technology, Management and Budget Resources

Issue Date: December 22, 2003

- SUBJECT:** Acceptable Use of State of Michigan Department of Technology, Management and Budget Resources
- APPLICATION:** All executive branch agency computer end-users; including employees, interns, vendors, contractors, and volunteers. State hosted application specific end-user-agents at county and local units of government. System and network administrators. Lead-workers, supervisors, administrators, and managers at all levels. DTMB Office of Enterprise Security (OES). All computing equipment, devices, systems, servers, and data networks.
- PURPOSE:** To identify acceptable use of State of Michigan information technology resources, to provide awareness of expected end-user behavior, and to safeguard IT data resources.
- CONTACT AGENCY:** Department of Technology, Management and Budget (DTMB)
Office of Strategic Policy.
- TELEPHONE:** 517/373-7326
- FAX:** 517/335-2355
- SUMMARY:** This policy identifies acceptable use of State of Michigan Technology, Management and Budget Resources, provides awareness of expected end-user behavior, and is also intended to safeguard IT data resources. This policy requires that end-users maintain respect for the privacy of protected citizen and employee information at all times. A cooperative effort from every employee is necessary to prevent misuse, eliminate the risk of liability to the State, and promote the efficient utilization of IT resources and information technology services.
- APPLICABLE FORMS:** None.
- POLICY:** A primary mission of the Department of Technology, Management and Budget (DTMB) is to provide and support end-user computing devices, systems, applications, and network communications resources. These resources are for the official use by executive branch employees to meet the daily operational and business requirements of departments, agencies, and the various boards and commissions of the State of Michigan. Information technology resources provided to employees are for the purpose of delivering public services to the State's diverse groups of customers in a more efficient manner. Employees should have no expectations of personal privacy protection when using State owned IT resources.
- PROCEDURES:**
Acceptable uses of IT resources include:
- A. Uses authorized by agency business units, with the exception of items listed in this policy.
 - B. Personal use by employees for interaction with human resource, time accounting, compensation, and employee benefits and health administration programs managed by or administered for the State of Michigan.

Procedure Update: 04/18/06

Procedure 1460.00

- C. Access to information and transactions made available on the e-Michigan portals.
- D. Use of applications or access to information provided for general audience use on enterprise or agency intranet hosts.
- E. Access to Internet hosted on-line reference and information sources such as phone directories, on line dictionaries, or mapping and weather services if such use adds value to the business unit, increases employee efficiency, or legally avoids costs that would otherwise be incurred by the State of Michigan for such referenced services.
- F. Statutory and regulatory activities.

Unacceptable uses of IT resources include (but are not limited to):

- A. Any use of computer equipment that violates State or U.S. law and regulations are clear violations of acceptable use. The deployment, delivery, and use of technology resources within State of Michigan executive branch agencies is governed by statute and published procedures such as those contained in the DTMB administrative guide or within specific department and work group policies. Computer end-users and their direct supervisors must be aware of and be accountable for the elements of these laws, regulations, policies, and procedures as they affect daily work and responsibilities related to the use of IT resources utilized within their line of business work group.
- B. Creating or forwarding of chain mail regardless of content, sources, or destinations. Posting agency information to external newsgroups, bulletin boards or other public forums without authority.
- C. Using equipment for personal profit, political fundraising, gambling activity, non-business related instant messaging or chat room discussions, and downloading display of offensive material.
- D. Any use that violates public safety or compromises the privacy of legally protected resident or citizen information.
- E. Hacking systems and databases or acting to disrupt systems or cause unnecessary network congestion or application delays.
- F. Use of any remote control software on any internal or external host personal computers or systems not specifically set up by DTMB staff using methods authorized by standard or policy.

All employees or computer end users shall be made aware of this policy and educated about its content and the impact of violations of acceptable use criteria.

- A. Awareness and education:
 - (1) Each executive branch end user is required to acknowledge this policy.
 - (2) Log in screen reminders (appendix 1) are required for periodically reminding employees of this and similar policies directly affecting end-users. These reminders will be presented on screen prior to or during the logging in routine.
 - (3) IT training sponsored by the State of Michigan may include a segment on this policy and good cyber-citizenship.
 - (4) Application specific security rules and procedures mandated by State of Michigan and federal regulations must also be rigorously adhered to in order to safeguard legally protected data resources from compromise and should be a part of agency sponsored privacy and security awareness efforts.
 - (5) Every user should perform due-diligence measures to contribute to a professional, safe, pleasant, and non-offensive IT user environment. Remember: e-mail is subject to the Freedom of Information Act (FOIA). E-mail and other information may still remain on your PC after deletion.
 - (6) Violation of this policy may result in agency-administered discipline up to and including discharge. Criminal or civil action may be initiated in appropriate instances.

- B. Inadvertent and Erroneous use – End-users inadvertently directed to a web site that violates laws, regulations, or policies may claim erroneous use. Mistakes occur when using IT resources without any employee intent to violate policy. A claim of this type is only substantiated by connection times measured in seconds, rather than minutes when found in network, system, or application log audits done to verify or detect abuse. Report to supervisors or managers when un-intentional misuse occurs. Self-reporting is encouraged and may be done without consequence.

DEFINITIONS:

Agency - means executive branch entities including agency, department, board, or commission.

AIO - Agency Information Officer

Business Units - Supervised areas of related work responsibility as explicitly defined and delegated to them by executive branch agency directors, boards, or commissions of the State of Michigan.

Chain Mail - unauthorized non-government or NON-business related e-mail to large groups, the SOM address book, or to unspecific destination addresses that suggest that the receiver should further disseminate the message.

DTMB - Department of Technology, Management & Budget

Due Diligence - activities that ensure the protection mechanisms are continually maintained, operational and applicable to state and federal laws.

Employees or computer end-users - includes the broad range of persons who are supplied with any IT resources or application access by DTMB to accomplish State work and include all executive branch agency employees; including interns, vendors, contractors, volunteers, and agents at county and local units of government who are given password access to specific State of Michigan hosted applications.

Hacking - Gaining or trying to gain unauthorized access to systems and databases either internal or external to the State of Michigan computer systems or networks for the purpose of viewing, stealing, or corrupting data.

IT systems or resources - Data networks (over any media type); computer devices including: servers, hosts, laptops, desktops, handheld, or tablet pc; communication devices: phone, web phones, or pagers; and software applications accessed with any interface device.

Mass Mail - authorized State of Michigan business related e-mail to large groups or the whole SOM address book sponsored or originated within an agency business unit.

OHR - Agency Office of Human Resources

OES - DTMB Office of Enterprise Security

OUs (operations units) - describe any employee groups of DTMB functions supporting specific agencies and/or applications.

SOM - State of Michigan

RESPONSIBILITIES:

- A. Employee end-users – must read this document, understand the expectations and take personal responsibility for adhering to the provisions of this policy. Each end-user will be required to acknowledge receipt of this policy and any agency specific addendums. All categories of employees must realize that misuse or abuse of IT resources may lead to department or agency investigation and initiation of legal or disciplinary actions. Be aware that computers assigned to you may also be removed from your office area for analysis.
- B. Agents, contract staff, vendors, and volunteers – are required to adhere to this policy, acknowledge an awareness of this policy, however realizing the consequences of willful violation will be appropriate to their status.
- C. Supervisors, managers, or directors - make up the first line of accountability for staff compliance with this policy and shall require that all staff under their management read, and acknowledge the acceptable use agreement, and abide by the provisions of this policy.
- D. Agency OHR – shall support supervisors and managers as needed in the awareness and disciplinary enforcement of this policy.
- E. DTMB staff and OUs– shall report suspected violations to OES when found in the normal course of system support activity and assist OES with audits and enforcement actions when requested to do so.
- F. Office of Enterprise Security (OES) – shall receive and document reports of suspected abuse from any source and act as necessary on each reports.
- G. OES shall plan and supervise periodic system and network audits to detect potential abuse and shall use these audits to identify and investigate non-compliance with the provisions of this policy. Report incidents of abuse to agency DTMB AIO, agency OHR liaison, and agency internal auditor, and where abuse may involve criminal activity to appropriate State of Michigan or other law enforcement officials. Assist in the collection and preservation of digital forensic evidence when requested by law enforcement officials.
- H. Agency Business Units - shall ensure that all aspects of the IT Acceptable Use policy and standards are communicated to staff within their divisions and work groups.
- I. Contracts Management and Purchasing Division – Holds the responsibility to communicate acceptable use policy to vendors and contract staff that will be using IT resources, emphasizing the need for ensuring compliance with this policy. Purchasing process shall include contract language requiring vendors' staff to follow acceptable use policies, and require that all vendor staff acknowledge the acceptable use agreement.

EFFECT:

The policy described in this section sets a minimum level of conformance that will be implemented across the State of Michigan enterprise. Agency work rules should support this policy direction and provide departmental guidance on how violations will be handled. Work rules or policies that are consistent need not be reissued. State Departments desiring to implement more restrictive policies regarding information technology resources may do so by coordinating with OES prior to implementation.

Appendix 1

Sample Screen Acceptable Use Agreement login acknowledgement in Window or Banner:

I have read and am fully aware of the STATE OF MICHIGAN Department of Technology, Management and Budget Resources Acceptable Use Policy # 1460.00 I understand that I am expected to <u>act in accordance with this policy</u> when using State of Michigan computing equipment and applications at all times.
--
