Information Technology Privacy Policy

1.0 Purpose

Murray State University provides numerous information technology resources for the benefit of all members of the university community. These resources include frequently accessed programs such as web sites, email, course management systems, and online payment systems as well as computer systems such as myGate which may be more specialized in their use and application. Members of the public, too, may visit and search MSU web pages and utilize tools which appear there. The University also provides network and internet access thru the Campus and ResNet networks to members of the campus community. Of course, MSU also provides numerous computers for use with work and study as well as the basic infrastructure and architecture which enables the system to operate.

All of these resources enable users to communicate with each other, the University, and others off campus; to transact various matters of business; and to gain access to a vast amount of data with greatly increased ease and efficiency.

MSU has established this policy so that users are aware of the privacy which surrounds their use of technology resources and the information and communications they send and which are received by, and which are stored in, such means.

If you have any questions or concerns about this policy or your information, please contact Information Systems at 809-2155.

2.0 Scope

This policy applies to all users of university information technology resources, which is defined as all information technology/network equipment, facilities, and services made available to users by Murray State University, and the data stored thereon. The term information technology resources encompasses all university owned and operated computers, software, hardware, and infrastructure. It further includes all university services and programs such as email, online payment, and MSU web pages. It also includes:

1. Data and other files, including electronic mail, stored in or located or residing on (temporarily or otherwise) university-owned centrally-maintained systems, departmentally-maintained systems, and university-owned systems or computers.
2. University data and other files stored off campus in systems owned or operated by other entities. These systems may be subject to their own terms and conditions related to privacy and other matters.
3. Data communicated over Campus and ResNet networks.
4. Telecommunications (voice or data) traffic from, to, or between any devices described above including voicemail.

As used in this Information Technology Privacy Policy, “you” and “user” both refer to any individual -- whether student, faculty, staff, or individual external to MSU -- who uses MSU information technology resources.

3.0 Policy

3.1 What Information is Available from MSU’s Technology Resources

3.1.1 Information You Knowingly Provide

You may communicate via Murray State's information technology resources for many reasons. You may send an email to the Bursar's Office, Human Resources, a work colleague, or a friend; forward a draft document to a co-worker; submit a class assignment to a professor electronically; or apply for admission to the University via an online form. Thus, depending upon the nature of any communication the information transmitted and available through information technology resources could include personally identifiable information such as name, telephone numbers, date of birth, permanent addresses, social security number, employment or class information, etc. Information requested by MSU in forms or applications is needed so MSU can provide the service you need or request.

3.1.2 Information You May Not Realize You Provide

In addition to the kinds of information referenced above, information may be transmitted and recorded (whether you realize it or not) anytime you use Murray State's technology resources including simply visiting a Murray State University web site. This information includes but is not limited to:

- Internet address of the computer being used
- The web pages requested or viewed
- The network software accessed
- The web page which referred the user to any MSU web page
- The internet browser used
- The date, time, and duration of the activity
- The accounts accessed
- The volume of data stored and transferred

3.1.3 Documents and files

You may use MSU's information technology resources to create files, documents, or other compilations of data or information. These items may not be sent to anyone, but may simply be created on a MSU computer at a work station or in a computer laboratory and could remain there without you intentionally saving them on the computer.

MSU's information resources are used to create, store, and manage files or documents about employees, students, alumni, contractors, and others. These documents can contain personally identifiable information including name, address, date of birth, social security number, gender, race, grades, and other personal information, as well as financial information such as salary, banking information, and payroll deductions. Such information and the compilation of such information are necessary in order to carry on the regular operations of an institution of higher education.

3.1.4 Cookies

Cookies are a technology which can be used to provide you with tailored information from a web site. A cookie is an element of data that a web site can send to your browser, which may then store it on your system. It can then be read back later by the web site when required. The use of cookies is a convenient way of allowing a computer to remember specific information relating to a web site. You can set your browser to notify you when you receive a cookie, giving you the chance to decide whether to accept it.

MSU's systems make use of cookies for the following purposes:

- Site administration
- Completing the user's current activity

- User Targeting

3.1.5 Information from On-Line Payments

It is possible to make on-line payments at MSU with debit and credit cards and e-checks. In some instances, the user making the payment is directed to a third party website in order to make payment. The third party sites may have their own privacy policies. In other instances, on-line payments result in the storage of information on MSU servers.

3.1.6 E-Mail

Emails sent or received using MSU's information technology resources or sent from or to any email address provided by MSU (eg. astudent1@murraystate.edu or astudent1@coe.murraystate.edu) are subject to monitoring and access by MSU.

MSU may utilize an outside e-mail/service provider. In the event MSU utilizes an outside e-mail/service provider, MSU will maintain on its own servers copies of all e-mail sent or received through that e-mail/service provider; this email will be subject to this Information Technology Privacy Policy. The e-mail/service provider will also monitor and have access to the accounts which it provides. MSU will also have access to emails and other documents/transmissions in those accounts maintained by the provider. The provider will have its own privacy policies.

3.2 Who Has Access to Information Available From MSU's Information Technology Resources?

3.2.1 MSU Employees

1. To provide services
    - As noted above, information technology resources are used to communicate with the University and its staff and faculty for many different reasons. Requests for services and information from and submissions to the University are reviewed by the appropriate MSU employee. Depending upon the nature of the user's transmittal, the communication may be reviewed by more than one employee in order to provide the needed service. These employees will only use this data for work related purposes, which may include sharing it with appropriate individuals outside MSU, and as otherwise allowed here.
    - In the course of their normal job duties and the operation of the University, authorized employees will have access to data, including stored data, about you. This data may not have been communicated directly to those employees by you, but appropriate employees will have access as a regular part of their employment. They will only use this data for work related purposes, which may include sharing it with appropriate individuals outside MSU, and as otherwise allowed here.
2. Monitoring and Access
    - MSU, as a regular part of its business, monitors its information technology resources in an effort to ensure they are used in accordance with law and university policy, that they are operating efficiently, that there are no threats to them, and that they are regularly maintained and up-dated. This regular monitoring may result in MSU's accessing information technology resources you use including email and communications you send or receive, viewing or scanning files or software you have placed on MSU's information technology resources, and retrieving, copying, and

distributing information found. Appropriate action will be taken if this regular monitoring reveals violations of law or any university policy.

- MSU may as a regular part of its business also monitor and access the information technology resources you use. This includes email and communications you send or receive or files or software you have placed on MSU's information technology resources. MSU may retrieve, copy, and distribute information found if such actions are taken by an employee as a regular and necessary part of his/her job duties, or if such actions are determined to be in the best interests of MSU by the Chief Information Officer or higher level of university management. This may occur, for example, in the event there are reasonable grounds to believe:
  - There is a threat to the University's information technology resources, or if such access is needed to ensure the efficient operations of any MSU information technology resources
  - That a violation of university policy or an illegal act has occurred or may occur
  - There is a threat to university property or the rights of the University
  - There is an emergency affecting the safety of persons or property
  - Access is needed in order for MSU to conduct its regular business affairs efficiently
  - Litigation involving the University or its agents or employees is possible or on-going.
  - A work document, to which a department needs access, is on an employee's computer but the employee is absent.
- MSU's monitoring and access may occur without notice to you. The fact that any information technology resource is password protected will not prevent monitoring and access by MSU. Monitoring and access may include physically accessing information resources wherever located.

3.2.2 Disclosure of information to individuals outside of MSU

1. MSU may initiate disclosure of information from its information technology resources to persons or entities inside or outside the University if needed in order for MSU to carry on its activities as an institution of higher education or if otherwise consistent with law. MSU employees may need to share information with other agencies in order to implement programs provided at MSU or to assist with a particular request. MSU will advise law enforcement officials, including the University's Department of Public Safety and Emergency Management, if the regular monitoring of its information technology resources uncovers activity which may be criminal in nature such as downloading child pornography or communications of an illegal nature.
2. Requests for information from persons or entities outside the University. The following considerations are relevant in the event MSU receives a request from a person or entity outside the University for information, including personally identifiable information, available from its information technology resources.
   - FERPA. In general, personally identifiable information in records maintained by or for MSU which directly relates to a student may be disclosed only as allowed by the provisions of the Family Educational Rights and Privacy Act (FERPA). The University's current FERPA policy, including the provision by which students can prevent disclosure of certain "directory information," can be found at http://www.murraystate.edu/Academics/RegistrarsOffice/FERPAPrivacyAct.aspx In addition to what is stated in the policy, FERPA recognizes that information in student records can under certain circumstances be shared with individuals outside MSU even if a student does not consent.

- Kentucky Open Records Act
  - Because MSU is a public agency, it is subject to the provisions of the Kentucky Open Records Act. These statutes require the release of certain records the University maintains, including electronic records, if a proper request is made.
  - Not all records, however, are subject to release. The open records act exempts from disclosure, for example, information of a "personal nature" contained in a record maintained by the University. Thus, MSU does not provide an employee's social security number or bank account information even if a proper open records request regarding the employee is made. Information otherwise protected from disclosure by FERPA will not be disclosed in response to a request under the Open Records Act.
  - Employee users of MSU's email system are advised that their private and business email communications may be subject to the Open Records Act.
- Other considerations
  - Release of information found within MSU's information technology resources may be required if it is the subject of legal process, such as a subpoena, or is requested by an agency with proper jurisdiction.
  - MSU may be required to produce information stored within its information technology resources in the event of litigation. In addition, MSU reserves the right to collect and release any information regarding or created by any user in the event MSU and the user are involved in litigation including any administrative or internal proceedings.

3.3 Security of information

Murray State utilizes appropriate and reasonable measures to protect the security of its information technology resources. It cannot, however, guarantee absolute security for information.

MSU has no control over the privacy of information you share on any pages or sites outside of the murraystate.edu domain even if they are accessed through or linked to MSU information technology resources. Similarly, MSU cannot guarantee security of data once it is released to a third party.

4.0 Review and Modification

1. Proposals for amendments to this policy will be forwarded to the Chief Information Officer. The proposals and comments will be brought before the ITAC Policy Review Subcommittee by the Chief Information Officer.
2. Any amendments to this policy will be approved by the President of the University. All new or amended policies will become effective as soon as Presidential approval is obtained and they have been published on the Policy website.

5.0 Penalty

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Acceptance/Consent

Signature on an account application form, acceptance of a user ID, online registration, or use of any information technology resource denotes that the applicant/user has read and understands, accepts and

consents to this Information Technology Privacy Policy.

Information Technology Privacy Policy (downloadable PDF)
Requires Adobe Acrobat Reader