NETWORK, EMAIL and INTERNET POLICY

The Minneapolis Institute of Arts (the "MIA" or "Museum") maintains an internal computer network, including Internet access and an electronic mail system ("email") for conducting MIA-related business and research. This policy governs appropriate use of the MIA's computers, network, email, and Internet access by all individuals, including but not limited to employees, interns, temporaries, casuals, contractors, and volunteers. Every individual whom the MIA grants an account on the Museum's network and/or email system is required to read and sign an acknowledgment of policy receipt and comply with this policy. A summary of this policy is also posted by all general-use computers.

ACCESS

Individual network accounts and/or email mailboxes will be provided to those who require it for the performance of their MIA job responsibilities. In order to obtain an account or use the network services, you must first agree to comply with the terms of this policy. You may not use the account or the network services if you do not accept the terms of this policy. By using the account or the services, you understand and agree that the MIA will treat such use as acceptance of the terms of this policy.

MONITORING, PRIVACY and INFORMATION OWNERSHIP

If you send or receive personal messages via web-based email services such as hotmail, gmail or yahoo mail using the Museum's network or email system, any of the information and/or messages stored, received, or transmitted are not private and they are not confidential. You should have no expectation of such privacy or confidentiality. If you want to keep your messages and information private and confidential, transmit them on non-MIA equipment and systems. All information generated, received, and stored on the Museum's computer equipment, including but not limited to servers, desktops/laptop computers, and removable media**,** is the property of the MIA, is accessible to the MIA and the MIA can access and use it in administrative, judicial, or other proceedings. The MIA reserves the right to monitor the content of network, email, and Internet activity in its discretion, particularly when a user is thought to be violating Museum policy or involved in illegal activity; when required by court order or law enforcement agencies; when there are health or safety issues; or when needed for system administration. The Head of Human Resources, the Deputy Director & COO, or the Museum Director & President can authorize the access to such information in such cases. If disagreements arise between an individual and MIA management regarding such access, the data in question will be secured pending an investigation and legal decision**.**

SECURITY OF INFORMATION

Since no computer system is completely secure, and may possibly be accessed by persons outside the system, all networked information should be considered unsecure. Private and highly confidential documents should not be transmitted, received or stored on the Museum's computers or network unless appropriate safeguards, such as passwords or encryptions, are used.

Email stored in the MIA email system is encrypted. Individuals sending confidential information via email must use good judgment that the recipient will properly protect the confidentiality of such information on any computer system on which the recipient stores the information.

Internal and external email messages, including messages sent or received via web-based email, may be discoverable in legal proceedings or investigations.

Any questions relating to appropriate security of information stored or transmitted on MIA computer systems should be directed to the Information Systems department.

An individual's use of the Internet, including web-based email, is neither confidential nor private as any information sent or retrieved on the Internet may be intercepted or recorded. Also, Internet Service Providers and Internet sites routinely monitor access and usage. Information stored on the MIA's computers, network, internal and external email messages (including messages sent or received via web-based email), and the record of Internet usage may be discoverable in legal proceedings or investigations.

Because computer systems are not completely secure, user names and passwords must be guarded by individuals. Individuals may be required to change their network access password on a periodic basis. Individuals are forbidden from sharing their passwords, accounts, or computers without authorization from the Information Systems department.

ACCEPTABLE USE OF THE NETWORK, EMAIL AND INTERNET

- Using email and the Internet for the Museum's business purposes, including academic research, professional communications, and locating information relevant to the MIA.
- Using email and the Internet for personal matters in an appropriate and limited manner that does not interfere with their job responsibilities, productivity or use of the resources for the Museum's business.
- Downloading of any type of file from the Internet is restricted to business related information files. Prior authorization from the Information Systems department is required before downloading business related software or program files.

UNACCEPTABLE USE OF THE NETWORK, EMAIL, (including web-base email) AND INTERNET

Unacceptable use includes, but is not limited to, the following:

At all times:

- Accessing personal or business audio-video material on the Internet that is not related to the business needs of the MIA.
- Copying, distributing, or sharing copyrighted materials without authorization of the copyright owner except where such use is subject to the Fair Use Doctrine as defined by U. S. copyright law (sections 107 through 118 of the Copyright Act, title 17, U. S. Code). Do not make any assumptions that a use is a "Fair Use." Ask for advice from the Visual Resources department before proceeding. MIA policies and AAMD guidelines apply as well.
- Violating software license agreements or terms of use of any website or resource provided by a third party.
- Sharing personal or business related audio-visual material on the network that is not related to the business needs of the MIA.
- Downloading programs of any kind to your computer or the network without prior authorization from the Information Systems department. See the Desktop Software Standard Policies for more details.

- Accessing pornographic or sexually oriented materials or materials deemed by the MIA to be inappropriate given the context or setting.
- Discussing confidential MIA business in online forums.
- Propagating computer viruses.
- Participating in or facilitating computer or network break-ins or security probes.
- Promoting political or religious positions or activities and/or political campaigns.
- Accessing or distributing the passwords of others.
- Misrepresenting yourself as someone else when sending an email.
- Sending messages that are offensive, harassing, obscene, derogatory, discriminatory, defamatory or threatening to any individual or group.
- Sending sensitive or confidential information without appropriate security measures. (Contact Information Systems if you require additional information or assistance on security measures.)
- Wagering, betting, or selling chances.
- Using the system for personal gain.
- Using the system in any way that violates or aids in the violation of any law.
- Widespread distribution of messages in multiple inappropriate forums (sometimes referred to as spamming).

ALL STAFF EMAIL MESSAGES

All staff email messages will be posted on the Intranet by the appropriate Division head or their designee.

RETENTION AND DESTRUCTION OF MESSAGES

The email messages transmitted on the MIA's system remain on the system until all the internal recipients and/or the internal sender delete them. Email and networked information may be retained on the MIA's back-up or archive media by the MIA, even after a message or file is deleted or erased. Please refer to the guidelines for determining when to keep emails and the Document Retention and Destruction Policy posted on MIAnet for guidance on the deletion of email.

EMAIL BOX MAINTENANCE

Incoming messages may be returned to the sender if a staff member's allocated email box exceeds its capacity or if the message contains an attachment that exceeds the size limit established by Information Systems or the MIA's email vendor.

TERMINATION OF MIA RELATED RESPONSIBILITIES

Your network, email, and Internet access will be discontinued immediately when your employment at the MIA ends. At that time, either incoming email will be redirected to an appropriate staff member or the message will be returned to the sender.

ROLES AND RESPONSIBILITIES

All users who are given access to MIA computer resources are responsible for compliance with this policy and:

- Being responsible for maintaining the confidentiality of passwords associated with any account you use to access the network services. If you become aware of any unauthorized use of your password or of your account, you agree to notify the Information Systems department immediately.
- Knowing and complying with any other published supplemental policies related to the Internet and email policies including security policies.
- Limiting your personal use of the Internet and Email to reasonable and appropriate use that does not interfere with your job responsibilities, productivity or with business use of the resources.
- Observing all network security practices including passwords and use only passwords assigned to them.
- Not viewing or using information that they have not been authorized to access.
- Always communicating in a manner that is professional and respectful.

You are encouraged to report any incident of noncompliance with the network, Internet, and email policies to management.

Directors, Managers, and Supervisors are responsible for:

- Identifying and evaluating the business necessity and applications for their employees and that their employees are following the network, email and Internet policies.
- Ensuring that all individuals with computer access working in their respective areas understand the policy and the necessity to comply with it.
- Notifying management and the Human Resources department of all instances of noncompliance and participating in disciplining employees when necessary.

The Human Resources department is responsible for:

- Requiring individual policy awareness and sign-offs.
- Informing all employees who are given access to the computer network of this policy.
- Recommending disciplinary action up to and including termination of any employee who violates this policy.

The Information Systems department is responsible for:

- Providing access to MIA computer resources to an individual only after they have signed the Acknowledgement of Receipt of this policy.

COPYRIGHT AND TRADE MARK POLICIES

It is the MIA's policy to respond to notices of alleged copyright infringement that comply with applicable law (including, in the Unites States, the Digital Millennium Copyright Act) and to terminate the accounts of repeat infringers.

ENFORCEMENT

You agree that you are solely responsible for any failure to comply with your obligations under this policy, and for the consequences (including any loss or damage) of any such failure. Any person who abuses the privilege of using the computers, network, email, or Internet system will be subject to disciplinary action, up to and including the possibility of termination of employment, depending on the seriousness of the policy infraction. Illegal acts involving use of the network, email, or the Internet may also result in civil or criminal penalties.

REMOTE ACCESS

On occasion, the MIA may furnish remote access to its network and email. This access may include, but is not limited to, the MIA email system, remote access to the server network, synching of email and calendars to handheld devices, and providing use of laptops and handheld devices. Providing this remote access does not in any way authorize overtime or working off-site. Overtime and working off-site must be specifically approved by your supervisor in advance.

ACKNOWLEDGMENT OF RECEIPT

I have received my copy of the Network, E-mail and Internet Policy. I have read the Policy, and I understand and agree to comply with the Policy. I also understand that I should contact the Information Systems department or the Human Resources department if I have any questions or concerns about this Policy or my right to use the MIA's network.

_____

Recipient's signature

_____

Name (please print)

_____

Date