Shiloh Museum of Ozark History
Computer Use Policy

Approved by the Shiloh Museum Board of Trustees 1-10-08

OVERVIEW

The Shiloh Museum of Ozark History ("the Museum") maintains computer hardware and software systems to assist staff and volunteers in performing their official duties and to provide educational opportunities for its audiences. These systems, all components and contents, as well as other data stored on or transmitted by City-owned equipment, are the property of the Museum and the City of Springdale ("the City").

SYSTEM STANDARDS

Compatibility, portability, and transfer of work products are essential in a team environment. As a result, the Museum and the City maintain standards for operating systems and software to help ensure compatibility with existing systems and ensure that system requirements are met. Similarly, all potential purchases of hardware, software, and peripherals must be approved by the City of Springdale's Information Technology (IT) department through the Museum director, as must all disposals.

COMPUTER USE GUIDELINES

The director is responsible for confirming that only appointed individuals (City IT employees or – rarely – Museum staff members) may install computer hardware, software, and peripherals. All software must be screened for viruses by the installer. The director, through the City's IT department, is also responsible for confirming that IT and the Museum retain adequate computer documentation. All original installation CDs, DVDs, or diskettes will be maintained by the City's IT department, except for user manuals and media which may be maintained at the most appropriate work desk or, if not in frequent use, stored in the Museum's safe.

The unauthorized duplication and use of City-owned software and/or documentation is strictly prohibited. Software owned by or licensed to the Museum may not be copied or distributed over a network or copies provided to bulletin boards or other services without the written approval of the director.

Software (including personally owned software) that is not licensed to the Museum or City or that violates copyright law may not be loaded on any machine owned by the Museum or the City. Museum networks and individual machines may be reviewed at any time for the existence of unauthorized software. Any such software will be immediately removed.

All computer work, including word processing documents, databases, spreadsheets, and graphic designs, produced for the Museum, whether by Museum staff, volunteers, or paid consultants, is the property of the Museum and is licensed and protected under the law as Intellectual Property. Downloading of data files and Museum-owned software for work at home by Museum staff or selected volunteers must have the approval of the director before removal from Museum premises, and all returning work for uploading must be virus-free.

All computer work on the City's Q drive will be backed up by the City IT department daily. Museum staff members should only use their C drives for files they are comfortable losing and are responsible for making sure that their C-drive files are regularly placed on the Q drive for automatic back-up. The City IT department will also daily back up the collection and photo databases from the T drive to the Q drive. Museum staff members are allowed to make back-ups on CD, DVD, or other portable media but those back-ups should not be considered the Museum's prime source should files be lost. Such portable back-up media should be stored in the Museum's safe. Along with the collection and photo databases, the T drive should be used for sharing of files among staff (with the appropriate staff member removing files from the drive after being used) and for large files that are only occasionally changed (e.g., images used for publicity). The latter types of files should be downloaded to CD, DVD, or other portable media for back-up.

The City's IT department is responsible for equipping all computer work stations with virus protection software. It is the computer users' responsibility to assure that every disk, CD, DVD, USB drive, or other peripherals used are free from viruses before use on a Museum computer.

WEB SITE

The Museum maintains a Web presence at a fully licensed electronic domain address connected to the City. Electronic products located on or licensed to other domain addresses are not authorized by the Museum and do not represent the Museum's views. All other electronic products produced by the Museum are the property of the Museum and are licensed and protected under the law as Intellectual Property. The director will appoint a staff member responsible for Web site maintenance and updates; no other individual except the director is authorized to alter the Museum's web site without the director's permission.

EMAIL AND INTERNET USE POLICY

The Museum provides many computing resources for use by staff. Staff are encouraged to use electronic mail, or email, and the Internet for Museum-related activities and to facilitate the efficient exchange and gathering of useful information. Access to email and the Internet is a privilege and certain responsibilities accompany that privilege. Users of email and the Internet are expected to be ethical and responsible in their use. While the City's IT department routinely blocks access to certain web sites, staff are strictly prohibited from viewing inappropriate web sites. Should such a site accidentally open, staff members should immediately notify the director.

EMAIL AND INTERNET USE GUIDELINES

Access to and the responsible use of modern information resources are essential to the pursuit and achievement of excellence at the Museum. The Museum encourages appropriate use of email and the Internet to enhance productivity through the efficient exchange of information in furtherance of education, research, public service, and the expression of ideas. Use of these resources must be consistent with these goals. Museum staff and volunteers are expected to act in accord with the following general guidelines based on common sense, common decency, and civility applied to the computing environment.

Messages sent as electronic mail must meet the same standards for distribution or display as if they were tangible documents. Users must identify themselves clearly and accurately in all electronic communications. Alteration of the source of electronic mail, messages, or postings is

unethical and possibly illegal. All incoming electronic mail files must be assumed to be private and confidential unless the owner has explicitly made them available to others.

No computer security system can absolutely prevent a determined person from accessing stored information that they are not authorized to access. While the Museum has no interest in regulating the content of electronic mail, it cannot guarantee the privacy or confidentiality of electronic documents. Good judgment dictates the creation of electronic documents that may become available to the public. Electronic documents which are expected to have extended use must be archived to computer hard drives and deleted from email files.

All users must respect the rights of others. No abusive, threatening, or harassing materials may be sent. No use may interfere with others' work or disrupt the intended use of shared resources. Users must especially avoid wasteful and disruptive practices such as sending "chain letters." Email and the Internet may not be used for commercial purposes or for personal financial gain.

The same standards of conduct expected of staff and volunteers regarding the use of telephones, research materials, and other institutional resources apply to the use of email and the Internet. Users are expected to abide by the security restrictions on all systems and information to which they have access. Users must avoid any communication where the meaning of the message, or its transmission or distribution, would be illegal, unethical, or irresponsible. Conduct which involves the use of information resources to violate a Museum policy, or to violate another's rights, is a serious abuse subject to appropriate disciplinary action. No Internet site which charges use fees may be accessed by Museum staff or volunteers unless it has been authorized in writing by the director.

While valuable Museum and City resources are involved in the overall operation of Museum computer systems, the use of email and the Internet for personal messages and information does not ordinarily result in additional costs to the Museum. However, as with telephone use for private matters, this use must be held to a minimum, must not interrupt or interfere with daily work activities, and must always be subordinate to Museum-related matters. The director has the authority to limit personal use of email or the Internet.

PASSWORDS

Each staff member is assigned an individual password for network access. Users should keep the director apprised of current passwords, but passwords should only be shared with other staff members on a need-to-know basis. Passwords should not be posted or easily visible by others. Users should not share personal passwords with volunteers or visitors. On a semi-regular basis, but always following any security lapse, staff members should change their passwords

DOCUMENT RETENTION AND SECURITY

The City and Museum adhere to the requirement of the Sarbanes Oxley Act, under which required information must be preserved for five years. This includes all correspondence, contracts, emails, and other documents that have a bearing on the financial picture of the Museum. If there are questions about whether a specific document falls under this policy, please consult the director.

All documents containing social security numbers, other personal information, or Museum financial data should be kept in a secure environment.