

## **Oregon State Library Policy Implementation Guidelines Information Asset Use, Implementation, and Security**

These Guidelines describe the implementation of a variety of statewide policies at the Oregon State Library. The main policies included are:

- *Acceptable Use of State Information Assets* (107-004-110), effective 10/16/2007
- *Controlling Portable and Removable Storage Devices* (107-004-051), effective 7/30/2007
- *Employee Security* (107-004-053), effective 7/30/2007
- *Information Asset Classification* (107-004-050), effective 1/31/2008
- *Information Security* (107-004-052), effective 7/30/2007
- *Information Security Incident Response* (107-004-120), effective 11/10/2008
  - Implementation of this policy is covered by the State Library's *Information Security Incident Response Plan*, effective 4/30/2009
- *Transporting Information Assets* (107-004-100), effective 1/31/2008

Staff behavior related to these guidelines is also governed by:

- Statewide Policy: *Maintaining a Professional Workplace* (50.010.03), effective 8/27/2007
- Statewide Policy: *Telecommuting* (50.050.01), effective 8/1/2008
  - Implementation of this policy is guided by the State Library's *Telecommuting Agreement*, effective 1/1/2009
- *Restrictions on Political Activity by Public Employees* from the Secretary of State Elections Division, authorized under ORS 260.432
- OSL Policy: *Customer Service*, effective 1/10/2007
- OSL Policy: *Library Working Hours*, effective 11/27/2006
- OSL *Shared Values*, adopted 12/4/2007

### **1. Definitions**

#### **a. Information Assets**

Any knowledge that can be communicated or any written material that has business value, regardless of its physical form or characteristics.

#### **b. Information Systems**

Computers and their connected or peripheral hardware, software, networks, storage devices and media used to collect, process, store, share or distribute information assets.

#### **c. State Information Assets and Systems**

Information assets and systems that operate within or maintain any access beyond ordinary public connections to the state's shared computing and network infrastructure. For the State Library, this implicitly includes all information assets and systems operated by and for the Library in the conduct of its business and mission.

#### **d. Portable Devices**

Any information system designed or intended for easy transportation or quick compatibility with multiple other information systems. This includes (but is not limited to) laptop computers, PDA's, smart phones, USB storage devices, MP3 players, etc.

#### **e. Attachment**

Attachment of systems to other systems includes but is not limited to direct connection such as through a USB port, network connections either wired or wireless, and installation or downloading of software and files.

#### **f. Software**

Any program, application, or script that can be installed, loaded or run on an information system. For the purpose of these guidelines, this includes plug-ins, most upgrades, and optional tools that can be added to existing software.

#### **g. Staff**

Any employee of the Oregon State Library: permanent, temporary, or seasonal; full- or part-time, paid, unpaid, or volunteer.

## **Oregon State Library Policy Implementation Guidelines Information Asset Use, Implementation, and Security**

### **h. Work Time**

Work time is any time that staff are on work status and does not include breaks, lunch, or other incidental time that they may be at the work site before or after the work day. Details about work time are included in the State Library's *Library Working Hours* policy.

### **i. Insignificant Use**

Use of or access to state information systems that does not represent a significant burden on those systems. Burden includes time spent, bandwidth consumed, and any other reasonable measure of impact on the workplace.

### **j. Incidents**

An incident is any occurrence that violates State Library or statewide policies or guidelines, whether intentional or accidental.

### **k. Personal Information**

Any information which could clearly identify an individual or could compromise that individual's security or financial well-being, including (but is not limited to) social security numbers, credit card numbers, and banking and other financial account numbers.

### **l. Business Transactions**

Any activity that results in a transfer or transmission of personal financial information such as purchases, balance transfers, auction bidding, etc.

### **m. Automated Systems Unit**

The Automated Systems Unit (ASU) is the information technology section of the State Library and provides support and maintenance of Library information assets and systems.

## **2. Appropriate Usage Times for State Information Systems and Assets**

### **a. Work-Related Use**

State Library staff should primarily use state information systems and assets for work-related activities and to conduct their day-to-day business as employees of the state. Such use should occur during approved work hours as clarified in the *Library Working Hours* policy.

### **b. Personal Use**

Insignificant personal use of state information systems by State Library staff is only acceptable in the course of a regularly scheduled workday and if such use is:

- during the employee's break,
- during the employee's lunch time, or
- immediately (15 minutes or fewer) before or after the employee's scheduled work day. Note that such use is a courtesy to staff and does not in any way constitute work time or eligibility for overtime.

All use must be appropriate use as detailed in the relevant policies and in these guidelines.

## **3. Use of Personal Information Systems**

Personal information systems are any systems that are not owned and maintained by the state, regardless of their specific ownership. Limited use of such systems in the workplace is acceptable within the following parameters:

- Attachment (see definitions) of the personal system to the state system(s) must be approved by the employee's program manager in consultation with ASU as outlined in section 10. Use of the personal system must have either a legitimate business purpose or a reasonable personal purpose consistent with Appropriate Use (see 2b).
- The state system to which the personal system is attached must meet minimum security requirements, including active anti-virus protection.
- Attachment to state systems should only occur when such connection is required to use the personal system. Personal devices that require charging should be connected to electrical outlets rather than to ports on state systems.

## **Oregon State Library Policy Implementation Guidelines Information Asset Use, Implementation, and Security**

- Note that a system includes software; as such, any software downloads or installations must conform to these guidelines. Any software not provided by the Library is considered personal even if its implementation is related to the business of the agency. Staff wishing to acquire additional business software should consult with their manager as outlined in section 10.

### **4. Use of Networks**

#### **a. State-owned**

All state networks are state information systems and their use is governed by the relevant policies and guidelines. State networks – including but not limited to email systems, local area networks, file sharing systems, local domains, and internet access through wired or wireless networking – should be used only for work-related purposes or insignificant personal use.

Use of state-owned networks fits into the following categories:

- Administrative – full access and control, limited to ASU and key staff for specific functions.
- Staff – full, unrestricted access to networks subject to these guidelines and relevant policies.
- Patron – restricted access to the internet and no access to the Library domain, available at the computers in the reference room.
- Guest – access to internet only, available with a guest logon and password through wired or wireless connections throughout the building.

#### **b. Personal or Commercial**

Library staff may have personal information systems (such as smart phones) that have access to their own, non-state networks. Use of these devices:

- should be limited to the timeframes identified in section 2b – Personal Use.
- need not be insignificant use and is not restricted by many of the limitations placed on state systems since there is no direct impact on or security risk to state systems.
- must still conform to appropriate use regarding maintenance of a professional workplace and restrictions on certain activities on state property (such as gambling, pornography, and illegal activities).

### **5. Use of Internet Resources**

In general, approved use of internet resources must be consistent with the appropriate guidelines regarding usage time, personal systems, and networks. Some internet activities are restricted or prohibited to protect network security and to prevent transmission of personal information across state systems. Employees may never use state systems for any activity that transmits their personal information, regardless of the presumed security of the target site. Particular internet activities that need special clarification include:

- **Prohibited Activity** – staff may never access gambling or gaming sites, pornography or other gratuitously sexually explicit sites, hate sites, or sites conducting illegal activity while on state property or during any work time, regardless of the information system used. This includes access to sites and any downloading or use of file attachments. Employees may never use state systems for any activity that transmits their personal information, regardless of the presumed security of the target site.  
If employees feel they have a legitimate business (e.g., research) need to access a site that fits one of these definitions, they must request and receive written permission from their manager *in advance* of accessing the site(s) and must provide a complete report of any activity on such sites after the business need is completed.  
If accidental access occurs, employees must immediately notify their manager with details of the access.
- **Business Sites** – staff may view financial information, bank balances, basic stock values, real estate listings, etc. as part of insignificant personal use. Staff may not conduct financial or business transactions using state information systems at any time and may not conduct financial or business transactions using personal information systems while on work time.
- **Shopping Sites** – staff may visit shopping or auction sites (such as Amazon.com, eBay, or Target.com) as insignificant personal use for the purpose of viewing merchandise or services. Staff may not conduct business transactions on these sites using state information systems at any time nor on personal information systems during work time.  
Staff with a legitimate business need to perform transactions on such sites may use a Library or other state provided account to make purchases within the scope of their position descriptions.

## **Oregon State Library Policy Implementation Guidelines Information Asset Use, Implementation, and Security**

- **Personal Gain** – staff may never use state systems nor use personal systems while on work time to conduct business (including selling items or services online) that results in any personal gain or profit.
- **Political Activity** – staff may not engage in any political activity using state systems or on work time. Any political activity is defined in and must conform to the restrictions issued by the Secretary of State Elections Division.
- **Polls and Surveys** – staff may not use state systems to participate in polls and surveys at any time unless the poll or survey is business related. Participation in polls and surveys on personal systems is permitted when such activity conforms to all applicable policies and these guidelines.
- **Music and Video** – staff may play music (within the limits of the customer service and professional workplace policies) from CDs or DVDs on state systems or using personal systems that do not connect to state systems. Software and systems used to play music must conform to these guidelines. Staff may not use state systems to download, share, purchase, or transfer (including burning of discs) music or video files even during non-work time. Staff may play streaming radio, audio, or video for work-related purposes or for personal use which conforms to these guidelines and creates minimal impact on the workplace. Staff may view videos related to their work using state systems and software conforming to these guidelines. Playing of personal videos on state systems is subject to the same restrictions as music and must not be done during work time.
- **Personal Email and Websites** – staff may access and view personal email or websites using state systems as long as such use conforms to all applicable policies and to these guidelines. Staff may send and receive emails from personal accounts when not on work time but may not use personal email to transfer files to or from state systems. Staff may not perform any maintenance on, uploads or postings to, or business using personal websites on state systems or during work time.
- **Social Networks and Sites** – social/networking sites (such as Facebook, Twitter, MySpace, and LinkedIn) can be useful for conducting the business of the Library. Staff with a legitimate business need to maintain professional networks and communications using such sites should establish an account associated with their state email. These accounts must be clearly for business purposes separate from any personal account or activity. Staff must request and receive written permission from their manager in advance of creating business-related accounts. Staff must limit any non-business-related use of or access to social/networking sites as personal use described in 2b. Use of such sites on state networks must conform to all other guidelines, including content, language, transfer of files, conduct of business, etc. Use of such sites on personal networks on state property must conform to customer service and professional workplace policies. Staff should be cautious and professional in postings to such sites regarding the workplace. Such postings may be actionable under the professional workplace policy regardless of the time or location of the posting. Staff should consider the impact of their references to the workplace and their colleagues and exercise good judgment in any forum that may be publicly accessed.

### **6. Use of Electronic Communication Tools**

#### **a. Outlook email and calendar**

All Oregon State Library team members will:

- use Outlook as their platform for work email and for their shared electronic calendar.
- check their email several times a day.
- keep Outlook consistently open or use taskbar alerts for ongoing message notification as job duties require.
- respond to messages within one business day.
- check their email remotely when appropriate during work time (e.g., telecommuting, conferences, etc.).
- use the out-of-office option and coordinate with other team members for email management when unavailable to check and respond to email.
- let customers know when they hand off email requests to another team member.
- ensure that messages are readable by the widest range of email systems and adherent to accessibility standards as much as possible:

## **Oregon State Library Policy Implementation Guidelines Information Asset Use, Implementation, and Security**

- Emails have high contrast between the text and background (preferably black on white); alternate colors that maintain high contrast can be used for emphasis or to identify comments and responses within a reply.
- Emails should be formatted in rich text or plain text and should not include inline images.
- Staff should not use any “wallpaper” or other background formatting on their emails. For special internal-only messages (staff event invitations, etc.) reasonable use of wallpaper or moderate background colors and images is acceptable.
- ensure professionalism and attention to customer service needs:
  - Maintain a consistent, professional appearance and tone in your email messages.
  - Check for and correct spelling and typing errors in your messages.
  - At least for outgoing messages, use a signature block that includes at least the following: Name, Title, “Oregon State Library”, Phone number, and Email address. Other information may be added if relevant to contact, including street address, fax number, and alternate phone number(s).
  - Personalized sayings, if used, must be approved by the Program Manager and included after the signature block.
- use Outlook calendar to track all meetings, leave, and other obligations.
- make calendar entries clear and meaningful.
- use Outlook to schedule formal meetings with other library team members.
- respond promptly to Outlook meeting invitations.
- provide explanation and offer alternatives when unable to accept a meeting invitation.

### **b. Voicemail**

All Oregon State Library team members will:

- maintain current availability information on their voice message and update the greeting to reflect schedule changes.
- use the same password (1111) for access to the phone message system. Management may use alternate passwords which must be logged with the HR manager for emergency access.
- respond to voicemails in a timely manner consistent with the State Library Customer Service policy.
- forward calls responsibly – to someone who is knowledgeable and available to answer the phone (e.g., reference desk).
- maintain voicemail in accordance with the State Library Telecommuting policy and agreement.
- return voicemail messages that request a response within one business day.
- maintain adequate space in their voicemail box for incoming messages.

Each team will establish procedures for how to update phone greetings for absent or ill team members. Remote access to voice mail is available for approved work at home, or for travel and emergencies.

### **c. Instant Messaging**

All Oregon State Library team members will:

- use the common IM platform (Spark), either from a pc-installed client or the browser-based interface.
- log in to Spark at the start of the workday and remain logged in until the end of the workday, regardless of workplace (i.e., regular work at the library, telecommuting, or use of a fixed remote workplace). Staff are not expected to log in to Spark when attending offsite meetings, conferences, trainings, etc.
- update their status regularly to indicate availability. Recommended settings include:
  - AVAILABLE – default when working at one’s desk
  - AWAY – for in-house meetings, breaks, lunches, desk shifts, etc.
  - ON PHONE – when on the phone, attending web training, staffing L-Net, etc.Staff may add customized explanation statuses (e.g., “In a meeting” or “At lunch” as long as they are brief, clear, and professional in tone). Staff who are telecommuting must use the custom status “Telecommuting” under “Available” during their telecommute time.
- maintain an active list of Spark contacts appropriate for their duties. At a minimum, staff will include all members of their team and of any committee(s) to which they belong on their contacts.
- respond promptly when receiving an IM from another employee.
- clearly indicate when the IM conversation is complete.
- use email or other file-sharing tools (not Spark) to send attachments.

## **Oregon State Library Policy Implementation Guidelines Information Asset Use, Implementation, and Security**

Staff should remember that IM is set up for internal, business-related communications only. In keeping with state policy, Spark accounts set up for Library use may not be used for any personal messaging. As a state information asset, any communications using IM are considered part of the public record and are logged and stored by ASU.

### **d. State Library Online Sites**

Official Library sites include the State Library presence on Oregon.gov and GovNet, the State Employee Information Center (SEIC), PLINKIT, OSLIS, and the shared catalog of the Hatfield Library Consortium.

- Posting and editing content on these sites is handled on a team-by-team basis, with responsibilities and permissions coordinated by the appropriate manager.
- The Library Administrative Services (LAS) team manages the top-level Oregon.gov content.
- The Website Quality Improvement Committee coordinates overall content review and look-and-feel issues for the Library's web presence in conjunction with Library Council and the Management team.
- Participation in Oregon.gov content management activities is performed according to DAS E-Government standards; a single point of contact (SPOC) for content management is assigned to a single staff person at the discretion of the GRS program manager.
- PLINKIT and OSLIS are maintained by Library Development. Other LSTA-funded online sites may be coordinated by Library Development as the need arises.
- The SEIC is maintained by the GRS Web Services Librarian as the coordinator of the Web Services Workgroup.
- The Hatfield Library Consortium is coordinated at the State Library by the Technical Services Librarian and the Cataloging Services Librarian in conjunction with the relevant Consortium committees.

Other websites, blogs, social networking sites, and online resources that fulfill State Library business purposes or represent the Library may be created as needed. Such sites must have managerial approval and a clearly identified purpose. Whenever possible, common statewide platforms should be used (e.g., the DAS E-Government content management system). Staff who edit, create, or maintain content on these online sites should:

- Have a clear understanding of the purpose of the site and ensure that any content is consistent with that purpose,
- Have sufficient training in the tools and software necessary to maintain content effectively,
- Have clearly defined responsibilities in their position descriptions related to the content or the maintenance activities, and
- Adhere to any other relevant policies, procedures and guidelines as they maintain the content.

## **7. Passwords**

Effective passwords are a critical part of information security. Access to email, voicemail, and the Library's network must be password protected. To ensure effective customer service and access to business information, staff will use a standard, agency-wide format, established by ASU, for their passwords. Exceptions to this standard are management, HR staff, and ASU administrative passwords for systems and servers. To obtain an exceptional password, employees must place a request with their manager, who will work with ASU if the change is approved. Any such exceptional passwords must be shared with the supervising manager.

Because other staff may need access to information stored on each other's systems, PC-specific passwords (such as those set on screensavers) are prohibited. However, laptops should have a machine-specific password for access when not connected to the OSL network to ensure security of hard drive content during travel.

## **8. Monitoring Behavior**

Managers have the right and responsibility to monitor use of state information systems. Monitoring may be done for cause or as part of a routine check. Managers will work with the ASU Coordinator to establish monitoring periods and parameters as needed. Any incidents discovered through monitoring will be handled as appropriate by the supervising manager.

## **9. Responding to Incidents**

## **Oregon State Library Policy Implementation Guidelines Information Asset Use, Implementation, and Security**

Most incidents will be resolved using the State Library's standard coaching and discipline procedures. Any suspected or actual incident should be reported to a manager immediately. Management will investigate the incident and take appropriate action.

Appropriate response to information security incidents is outlined in the State Library's Information Security Incident Response Plan. The primary contact for this plan is the Business Manager with the Human Resources Manager and the ASU Coordinator as backups. Library staff should notify one of the primary incident contacts whenever an incident arises or is suspected.

### **10. Decision-Making, Approvals, and Access**

As noted above, managers have the authority to approve use of state and personal information systems, installation of non-standard software for business purposes, and access to systems and networks as needed. An employee wishing to attach a personal system or download or install non-standard software will request permission from their manager in writing (print or email), describing the system and its business use. The manager will consult with the ASU coordinator as needed and make a decision regarding use of the system. Such consultation will include an analysis of any security risks, network impacts, support issues, and other issues related to consistency of network and system practices at the Library. Final decisions are at the discretion of management.

ASU maintains a list of approved software for use in the Library. Staff should use these programs since they have been vetted for security and functionality and are more familiar to ASU staff for support. Limited exceptions may be approved on a case-by-case basis. As described above, additional software may be purchased or downloaded for installation if there is a clear business reason for doing so.

In general, administrative access to Library systems is limited to ASU. Key staff may be given some administrative rights to specific systems as their jobs require. Such permissions should be agreed upon by management and the ASU coordinator and should be included in the appropriate position descriptions.