# POLICY 403 USING ELECTRONIC COMMUNICATION SYSTEMS

| | | |
|---|---|---|
| **Effective Date:** | June 1, 2011 | Number of Pages: 5 |
| **Modifies:** | June 1, 2010 | **See also:** Policy 101, 401, 404 and 407 |
| **Signed:** | Scott Jarvis | |

This policy applies to all employees and authorized users of the Department of Financial Institutions' (DFI) electronic communication systems. It defines and outlines proper and acceptable uses, prohibited uses, and privacy issues. When accessing electronic communication systems, particularly the Internet, employees represent the department; therefore all rules of conduct and law, which apply in the regular workplace, also apply to electronic communication systems.

This policy applies to all employees of DFI, including classified employees, members of the Washington Management Service (WMS), and exempt appointees. For purposes of this policy, authorized users include consultants, subcontractors, clients or any organization approved to access electronic communication systems through DFI.

**Definitions:**

**Electronic communication Systems.** All methods of electronic communication and information systems, including but not limited to, the Internet, news groups, bulletin board systems, Intranets, social media, computer hardware and software, programs, applications, and data, voice mail systems, telephones, faxes, electronic mail systems, video conferencing and transmissions, and other electronic media or devices that generate, store, transmit, or display information.

> **Note:** Electronic communication systems may not be secure from access by unauthorized persons, both inside and outside DFI. Letters, memos, e-mail, voice mail and Internet communications including social media all may be accessed without the knowledge or permission of the sender or intended receiver. In addition, most communications may be obtained through a public records request or subpoena. *[Employees should not communicate anything that they could not defend publicly as a business communication.]*

**Social Media.** Web-based technology that enables and facilitates rapid communication and/or networking through the Internet and/or cellular networks. Examples include:

- Blogs, and micro-blogs such as Twitter
- Social networks, such as Facebook and MySpace
- Professional networks such as LinkedIn
- Video sharing, such as YouTube and vlogs (video weblogs)
- Audio sharing such as podcasts

- Photo sharing, such as Flickr and Photobucket
- Social bookmarking, such as Digg and Delicious

## 1. Proper And Acceptable Use of Electronic Communication Systems Established

Employees or authorized users may use electronic communication systems in accordance with WAC 292-110-010 (Use of State Resources), if the use is reasonably related to the conduct of official state duties. Examples of acceptable uses are:

- Business communication with other DFI employees;
- Business communication with other governmental agencies, or industry or constituents;
- Gathering information on industry trends;
- Conducting legal or policy research;
- Gaining timely access to government publications and statistics; and,
- Investigative purposes.

Employees may make occasional but limited use of DFI provided electronic communications systems for office related functions. The following office related functions are approved by policy and do not require additional written approval:

- Combined Fund Drive (designated CFD coordinators only);
- DFI sponsored teams;
- Carpooling;
- Holiday events; and
- Adopt-A-Family

For office related functions not listed above, employees shall obtain written approval from the appointing authority prior to using DFI provided electronic communication systems.

DFI may authorize employees to use electronic communication systems and related materials to support or enhance professional growth activities.

Employees may make occasional but limited personal use of state e-mail and Internet resources if subject matter is not related to activities listed as prohibited and:

- There is little or no cost to the state;
- There is no interference with the performance of official duties;
- Is brief in duration and frequency;
- Does not distract from the conduct of state business; and
- Does not compromise the security or integrity of state information, state systems or software.

**Personal use of e-mail and the Internet during scheduled work hours is limited to five minutes or less, should be infrequent, and not every day. Employees may make occasional, but limited brief local phone calls. DFI considers these communications de minimis as long as performance of official duties is not affected. This does not include personal use of social media which is prohibited.**

Personal use of e-mail distribution lists is prohibited.

Examples of permissible e-mail and Internet use are given on the Washington State Executive Ethics Board Web site: **http://www.ethics.wa.gov**, in the Frequently Asked Questions section.
The terms of this policy applies to all uses of DFI communication systems. **SEE:** Policy 101, Outlining Agency Ethical Standards and Policy 404, Authorizing Use of Telephones and SCAN Access.

## 2. Electronic Communication Systems Prohibited Use Defined:

In accordance with WAC 292-110-010, the following uses of DFI electronic communication systems are prohibited:

- Any use for conducting an outside business;
- Supporting, promoting, or soliciting for an outside organization or group unless provided for by law or authorized by the Director or designee;
- Any campaign or political use;
- Commercial uses such as advertising or selling;
- Participating in non-business related chat groups, list servers or news groups;
- Sending chain letters;
- Allowing unauthorized access to protected state resources;
- Transmitting unprofessional communications;
- Viewing, storing, disseminating, or soliciting offensive or harassing material or statements, including any involving degradation of others based on their race, national origin, sex, sexual orientation, age, disability, and religious or political beliefs;
- Viewing, storing, disseminating, or soliciting material or statements including any which might incite violence or describe or promote the use of weapons or devices associated with terrorist activities;
- Viewing, storing, disseminating, or soliciting sexually oriented messages and/or images;
- Failing to honor copyright laws regarding protected commercial software and/or intellectual property; and
- Promoting any unlawful activity.

## 3. Social Media Prohibited Use Defined

Employees will use social media as a tool for approved agency purposes only.

Personal use of social media while on paid work time or using state equipment is prohibited. There is no de minimis use allowed.

Employees having a legitimate business purpose for establishing or posting to social media sites must request advance written approval from division management. Division management will notify the Chief Information Officer and the Communications Director of any approvals granted and the nature of such approval. Notification is not required when use is for regulatory investigatory purposes (e.g. searching). Employees will not use personal social media accounts for business purposes.

Employees will not represent themselves to be acting on behalf of the agency when posting to social media websites, or other online forums, unless authorized to do so by the Division Director or Agency Director.

Communications using social media may create public records that are subject to records retention requirements. Employees will discuss with management how such records will be retained prior to using social media.

Social media will not be used for unlawful or prohibited purposes as defined in Section 2 of this policy.

Social media shall not be used to distribute privileged or confidential material.

## 3. Managers Are Responsible For the Proper Use of Electronic Communication Systems Resources

Managers and supervisors will ensure that only authorized persons use DFI computer resources and related material, and only for acceptable and approved purposes. Internet use will be audited. Suspected inappropriate and/or prohibited personal use will be referred to the employee's supervisor and manager for disciplinary action.

## 4. DFI Retains Ownership Of All Computer-Related Material And May Access Data On Electronic Communication Systems

All computer-related material and all data created and stored on electronic data equipment are the property of DFI unless provided otherwise in an agreement. DFI may access data on any departmental electronic communication system without the employee's consent when necessary to carry out normal business functions, or if there is suspicion of possible misuse or violation of agency policy.

## 5. DFI Will Not Normally Disclose The Contents of An Employee's Files On DFI Communication Systems

DFI will not normally disclose to third parties the content of an individual employee's files except under special circumstances. Such circumstances include, but may not be limited to: a valid request for public records; a valid subpoena; or investigation of suspected misuse of DFI electronic communication systems, violation of DFI policy, or illegal activities.

## 6. DFI Discourages The Use Of Personal Email For Conducting Agency Business

Personal Email is any email account not issued for conducting DFI business. These can include email accounts such as: Hotmail, AOL, Gmail, Comcast Mail and others. Authorized email includes: DFI email, NCUA, ZixMail provided by DFI or one of our Federal counterparts. Any emails used in conducting agency business are subject to Electronic Discovery. If a DFI employee uses their personal email for conducting agency business then their personal email must be searched if relevant to electronic discovery or public records requests. If use of personal email to conduct agency business is unavoidable, the employee shall either CC: their DFI email address or ensure that they forward all emails to their DFI email address.
For questions related to electronic discovery see Policy 107- IDENTIFICATION, PRESERVATION AND DISCLOSURE OF INFORMATION.

Sending e-mails to or from an employee's personal e-mail to or from a DFI recipient including the employee themselves is acceptable. These e-mails are captured in the DFI e-mail archives.

## 7. Employees Using Electronic Communication Systems For Prohibited Purposes May Be Subject To Disciplinary Action

**SEE:** Policy 214, Correcting Performance and Behavior