Department of Financial Institutions

POLICY 403	**USING ELECTRONIC COMMUNICATION SYSTEMS**		
Effective Date:	June 28, 2019	Number of Pages:	7
Modifies:	June 1, 2011	**See also:**	DFI Policies 101, 106, 401, 407 & 408 WAC 292-110-010, http://www.ethics.wa.gov
Signed:			Charles Clark, Agency Director

This policy defines and outlines proper and acceptable uses, prohibited uses, and privacy issues regarding Electronic Communication Systems.

When using Department of Financial Institutions' (DFI) Electronic Communication Systems provided for official and authorized DFI business purposes, employees represent the department; therefore, all rules of conduct and law, which apply in the regular workplace, also apply to this policy.

All DFI employees and authorized users are covered by this policy and must comply with associated standards and guidelines.

Definitions

Electronic communication systems refers to all methods of electronic communications and information systems provided by DFI or the state of Washington, including but not limited to, the Internet, the Intranet, news groups, bulletin board systems, websites, social media, computer hardware and software, networks, programs and applications, data, telecommunications resources, electronic mail systems, and other electronic media or devices that generate, store, transmit, or display information.

Telecommunications resources refers to the following non-exhaustive list of authorized state-owned and state-controlled telecommunications systems and equipment:

- Mobile devices;
- Online collaboration (video conferencing, screen sharing, messaging, etc.);
- Voice mail, fax, and pagers.

Mobile device refers, but is not limited, to any DFI issued hand-portable device capable of text, voice, email, instant messaging ("IM"), photo messaging or other types of data communication. The mobile device definition is not meant to apply to: cars, boats, airplanes, laptop computers, desktop computers, unpiloted aerial vehicles (drones), Global Position System (GPS) receivers or radios.

Authorized account refers to any account issued by DFI or Federal partners for conducting DFI business. *Personal account* refers to any account for use or designed to be used by an individual for that person's own personal needs.

APPROVED
Executive Ethics Board
Date: 11-8-19

Authorized email refers to any email account issued or authorized by DFI for conducting DFI Business to include DFI email, ZixMail provided by DFI or one of our Federal counterparts. *Personal Email* refers to any email account not issued or authorized by DFI for conducting DFI business. These can include email accounts such as: Zoho, Gmail, Comcast Mail and others.

Authorized users are defined to include consultants, contractors and subcontractors, clients or any organization approved to access Electronic Communication Systems through DFI.

DFI employees refers to full-time, part time or temporary employees including interns and externs, classified employees, members of the Washington Management Service (WMS), and exempt appointees.

Internet Resources refers to the DFI systems, network equipment, software, and processes that provide access to and/or use of the Internet, including accessing, downloading, transmitting, or storing data and information, as well as the operation of software products and tools.

Network refers to wired corporate networks, wireless corporate and guest networks.

Objectionable material or statement refers to anything that could be reasonably considered to be obscene, indecent, harassing, offensive, or any other uses that would reflect adversely on DFI including but not limited to comments or images that would offend, harass, or threaten someone on the basis of his or her race, color, religion, national origin, gender, age, disability, sexual preference, or political beliefs.

Online Data Storage refers to the practice of storing electronic data with a third party service accessed via the Internet. It is an alternative to traditional local storage (such as disk or tape drives) and portable storage (such as optical media or flash drives). It can also be called "hosted storage," "Internet storage" or "cloud storage."

Social Media refers to online, network and Internet work based participating environments where users contribute commentary and electronic information that is available to the general public or privately to an audience consisting of more than the author contributor. Examples include but are not limited to:

- Blogs, and micro-blogs such as Twitter
- Social networks, such as Facebook and Instagram
- Dating apps or sites, such as Tinder, Hinge, Match.com, etc.
- Professional networks such as LinkedIn
- Video sharing, such as YouTube, Vine, and Snap chat
- Audio sharing such as podcasts, chirbit
- Photo sharing, such as Flickr and Photobucket
- Social bookmarking, such as Digg and Delicious

APPROVED
Executive Ethics Board
Date: 11-8-19

1. **Employees Will Limit Use Of Electronic Communication Systems To Approved Or Authorized Purposes.**

A. Approved Business Uses. 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. Note: Employees should not communicate anything that they could not defend publicly as a business communication.

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;
- Investigative purposes; and,
- Business Use of Social Media
    - 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 create a DFI social media account to conduct agency business.
    - Employees will use social media as a tool for approved agency purposes only.

Note: 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.

B. Other Approved Uses. Employees may make occasional but limited use of DFI provided Electronic Communication 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.

C. De Minimis Use. Employees may make occasional but limited personal use of state telecommunication systems, electronic communication systems, and other state resources only in the following circumstances:

- The use is limited to five minutes or less, infrequent and not every day;
- The subject matter is not related to activities listed as either objectionable or prohibited in Section 2., of this policy;
- There is little or no cost to the state;
- The use does not interfere with the performance of any state officer's or employee's official duties;
- The use does not compromise the confidentiality, integrity and availability of state information, state systems or software;
- The use is not for the purpose of conducting an outside business, in furtherance of private employment, or to realize a private financial gain; and
- The use is not for supporting, promoting the interests of, or soliciting for an outside organization or group.

Please see Appendix A for application of De Minimis Use to the State's Guest Wireless Network.

2. <u>Employees Will Not Use Electronic Communication Systems For Improper Or Prohibited Purposes.</u>

In accordance with WAC 292-110-010, the following uses of Electronic Communication Systems are prohibited:

- Any use for conducting an outside business;
- Commercial uses such as advertising or selling;
- 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;
- Participating in non-business related chat groups, list servers or news groups;
- Sending chain letters;
- Personal use of e-mail distribution lists;
- Transmitting unprofessional communications;
- Allowing unauthorized access to protected state resources;
- Viewing, storing, disseminating, or soliciting objectionable material or statements;
- 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;
- Failing to honor copyright laws regarding protected commercial software and/or intellectual property;
- Promoting any unlawful activity.

A. Prohibited Use of Social Media:

- Employees will not use personal social media accounts for business purposes unless authorized by a director.
- Personal use of social media, using state equipment, is prohibited.
- 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.
- Social media shall not be used to distribute privileged or confidential material.

B. Improper and Prohibited Use of Personal Accounts and Devices

- DFI employees must not use personal accounts or personal devices to conduct agency business, except as expressly authorized per DFI Policy 408, section F. REMOTE ACCESS.
- DFI data must not be stored in personal accounts or on personal devices.(see policy reference list)
- Mobile devices (DFI-owned or personal) must not be connected to DFI computers via USB or Bluetooth.

C. Improper and Prohibited Use of DFI Owned Mobile Devices

- All mobile devices must be equipped with an up-to-date, currently patched Mobile Device Management (MDM) or Enterprise Mobility Management (EMM) software.
- DFI employees may not send text messages (e.g. SMS, MMS, etc.) using unapproved text messaging applications on DFI-owned mobile devices.
- DFI employees may not use text messaging without prior director or division director approval (e.g. SMS, MMS, etc.) or instant messaging applications (e.g. instant messaging apps, WhatsApp, Viber, etc.).

3. DFI Managers, And Supervisors, With The Support Of The Chief Information Security Officer, Are Responsible For Ensuring Compliance With This Policy.

The Chief Information Security Officer is responsible for the development, implementation, and maintenance of this policy, associated standards and guidelines.

DFI managers and supervisors are accountable for ensuring that the "Using Electronic Communication systems" policy is communicated and understood within their respective organizational units.

4. Employees Rights And Responsibilities Regarding Electronic Communication Systems.

A. No expectations of privacy. Employees have no expectation of privacy when using state-owned Electronic Communication Systems. DFI and other State agencies reserve the right to monitor and review all activities and any content generated or received using Electronic Communication Systems and other state resources.

All records and all information created and stored on Electronic-Communication Systems, including the content of communications between DFI authorized users and a 3rd party, is the property of DFI unless provided otherwise in a written agreement. DFI may access any information, communications, records, or data created, stored, or accessed on any Electronic Communication System, without the employee's knowledge or consent, for any business function, including investigating suspected misuse of state resources or violation of state or federal law.

DFI reserves the right to disclose the nature and content of any user's activities involving Electronic Communication Systems and/or state resources to management, law enforcement officials, or other third parties without prior notice to the user, under certain circumstances. Such circumstances include, but are not limited to: a request for public records; a subpoena; or an investigation of suspected misuse of Electronic Communication Systems, violation of DFI policy, or violation of state or federal law.

B. Employees are responsible for mobile devices and all information and records on mobile devices. Each employee is responsible for mobile devices issued to the employee, including applying patches or updates as required by the Chief Information Officer or designee. Employees shall report lost or stolen mobile devices pursuant to Procedure 308E. Employees shall immediately return mobile devices to the employee's supervisor, program manager, division director, Chief Information Security Officer, or other agency leadership upon request.

C. Employees must create, retain, destroy, and otherwise manage records on mobile devices in accordance with DFI Policy 106. Employees will cooperate with the Public Records Unit and agency leadership, immediately upon request, to search and produce records and information stored on mobile devices, including any encrypted communications. If records and information cannot be searched and retrieved remotely via MDM or EMM software, the employee shall immediately return the mobile device to agency staff to retrieve records and information.

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

Failure to comply with the "Using Electronic Communication Systems" policy can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. See Policy 214, Correcting Performance and Behavior. In addition to disciplinary action by DFI, state employees may also be subject to action by the Executive Ethics Board under the Ethics in Public Service Act.

6. Employees May Request An Exception To The Policy.

Requests for exceptions to this policy must be submitted to the Director or Division Director and Chief Information Officer. Exceptions may be permitted after receipt of written approval from the Division Director.

Appendix A

De Minimis Use of the State's Guest Wireless Network

Purpose for the Guest Wireless Network (Wi-Fi)

The primary purposes for the Guest Wi-Fi are to provide wireless services for:

- DFI issued mobile devices
- Vendors and individuals visiting DFI who need Internet access for business related tasks
- Personal devices of employees while they perform business related tasks, such as taking an approved online college course during a lunch period.

How to Avoid Unauthorized Use of Guest Wireless Network (Wi-Fi)

DFI's guest Wi-Fi network is subject to De Minimis use…whether you are:

- Using a DFI device or your own personal device
- On a lunch period, a break, or at the office after working hours.

Treat the Guest Wi-Fi like any other state resource and follow De Minimis use rules. If you would not perform an activity on your DFI computer, you should not use the Guest Wi-Fi on a personal device to do that activity.

Streaming Internet radio like Pandora or Spotify, or streaming sporting events, entertainment, or any number of like uses does not satisfy De Minimis use and they consume state network resources intended for business purposes. These uses are prohibited while connected to DFI's Guest Wi-Fi, even on your own personal device.

Remember that your agency issued mobile device and personal devices may automatically connect to the Guest wireless network once you login the first time. ~~For standard but non-De Minimis use of your personal device, remember to first disconnect from the state wireless network and use your personal cellular service.~~

DFI intends to provide safe and efficient computing services for all our employees, and use state resources appropriately. Please contact your supervisor if you have any questions.

APPROVED
Executive Ethics Board
Date: 11-8-19