

# Vashon Island Fire & Rescue Operations Manual

Policy 9001:

Acceptable Use of Information Technology

Effective Date

06/24/2014

Approved and Issued:

06/24/2014

## 1.0 References

Code of Conduct

Washington Law against Discrimination

Title VII of the U.S. Constitution

National Labor Relations Act

HIPAA (Health Insurance Portability and Accountability Act)

Washington State Constitution, Article 8 Section 7. (Gift of Public Funds)

SOP 9002 Digital Imagery

## 2.0 General

This policy, along with the Code of Conduct, provides a common standard for the use of Vashon Island Fire & Rescue's (VIFR) Information Technology Assets to include workstations, Internet access, computer systems, websites including social media sites, email accounts, fax machines, cell or smart phone or other mobile devices and other new technology that may be implemented but not specifically addressed in this policy. The purpose of this policy is to provide guidance to members to clarify the boundaries between appropriate and inappropriate use of VIFR equipment and access, but may extend to communications through a member's home equipment and internet access by District personnel.

## 3.0 Purpose

It is the purpose of this policy to protect the confidentiality of members, patients and the public; to protect the careers of members, the reputation and resources of the District as well as District Operations.

## 4.0 Scope

This policy applies to all members of Vashon Island Fire & Rescue, unless specifically exempted.

## 5.0 Definitions

5.1 **Authorization:** The right or permission to use a computer resource.

5.2 **Authorized User:** A user with the right or permission to use a computer or technology resource.

5.3 **Computer Resources:** Any computer-based system available to a VIFR member. This can be a computer, database, network device, server, website, smart phone, printer, etc.

# Vashon Island Fire & Rescue Operations Manual

Policy 9001:

Acceptable Use of Information Technology

Effective Date

06/24/2014

Approved and Issued:

06/24/2014

- 5.4 **Information Asset:** A definable piece of information, information processing equipment or information system that is recognized as “valuable” to the Organization that has one or more of the following characteristics: Not easily replaced without cost, skill, time or other resources; and is part of the District’s identity, without which operations of the District may be adversely affected.
- 5.5 **Social Networking Site:** An online or web-based service that serves to promote connections and relationships with people, allowing message exchanges, posting of comments and photos or other digital images.
- 5.6 **Minimal Personal Use:** Brief in duration and frequency; does not interfere with or impair the employee’s ability to perform work; does not interfere with or impair the conduct of official VIFR business; results in negligible or no expense to the District; is not a prohibited use as described in Section 9.0 of this policy and has the appearance of professionalism even if it is not used in a public setting.
- 5.7 **System:** Software, hardware and interface components that work together to perform a set of business functions.
- 5.8 **User:** Any individual utilizing or affecting District computer resources or information technology resources, including, but not limited to, performing work for VIFR utilizing a personal computer, workstation, laptop or terminal, including, but not limited to, any employee contractor, consultant, or other worker.
- 5.9 **Member:** Employees, volunteers and other persons whose conduct, in the performance of work for the District, is under the direct control of VIFR whether or not they are paid by VIFR. This includes full- and part-time employees, elected or appointed officials, affiliates, associates, students, volunteers and staff from third party entities who provide service to VIFR.

## 6.0 Policy Statement – Being Identified as a Member of the District in Communications

- 6.1 Nothing in this policy is intended to restrict a member’s right to discuss as a private citizen, matters of public concern, nor engage in concerted activity with co-workers.
- 6.2 Members have an affirmative obligation to avoid being perceived as a spokesperson for the District.
- 6.3 Engaging in social media and social networking activities is a form of speech.
- 6.4 No member, while speaking as a private citizen on a matter of public concern regarding the fire district, shall speak in such a way as to cause harm or disruption to the operations of the District.

# Vashon Island Fire & Rescue Operations Manual

Policy 9001:

Acceptable Use of Information Technology

Effective Date

06/24/2014

Approved and Issued:

06/24/2014

- 6.5 Members may speak on a matter of public concern as a spokesperson for the District only with permission through chain of command. Members shall at all times exercise diligence to avoid holding themselves out as spokespersons for the District except when duly authorized.
- 6.5.1 The use of titles, VIFR logos, VIFR-owned images or identification as a member of the District that creates an impression that the member is a spokesperson for the District is prohibited.
- 6.5.2 Members are prohibited from publically discussing Fire District matters that are not of a public concern, unless doing so is with other employees and/or employee representatives and is for the purpose of engaging in concerted activities relative to workplace issues.
- 6.5.3 Members shall not engage in speech that is false, deceptive, libelous, slanderous, misleading or causes harm to others, including speech that constitutes hate speech or harassment; nor shall members discuss protected or confidential matters of the District, including matters that are under investigation, patient and employee information protected by HIPAA/medical confidentiality laws, or personnel matters that are protected from disclosure by law.
- 6.5.4 When engaging in social media or social networking activities, all personnel will maintain a level of professionalism in both on-duty and off-duty conduct that is consistent with the honorable mission of our District. The publication of any statement, comment, imagery or information through any medium of communication indicated herein, which is potentially adverse to the operation, morale, or efficiency of this department, will be deemed to be a violation of this policy.
- 6.5.5 Communication may include video chat while uniform/identifiable whether on or off duty and whether in full or partial uniform; using apparatus or stations as a backdrop; use of District owned digital images, audio, or video without District approval, in any way that may bring discredit upon the District or other members.

## 7.0 Policy Statement – District Owned Resources

- 7.1 VIFR provides its users with resources for the performance and fulfillment of job responsibilities. Prudent and responsible use begins with common sense and includes respect for the public's trust, the larger networked computing community and the access privileges that have been granted. The use of such resources imposes certain responsibilities and obligations on users and is subject to VIFR policies and applicable local, state and federal laws. Prohibited use of computing and technology resources can lead to

# Vashon Island Fire & Rescue Operations Manual

Policy 9001:

Acceptable Use of Information Technology

Effective Date

06/24/2014

Approved and Issued:

06/24/2014

consequences affecting the individual user, many other users and can cause service disruptions and/or loss of assets.

## 7.2 Applicability

This policy applies to all VIFR members, whether full-time, part-time or temporary employees, volunteers, and other individuals who are provided access to the District's technology resources.

## 7.3 Ownership and Audits

All equipment contained in the District's computer system is either owned, leased or subscribed to by the District. The District reserves the right to conduct random and requested audits or inspections of employee accounts in order to ensure compliance with policies and law, to investigate suspicious activities that could be harmful to the organization, to its systems or vital data, to assist supervisors in evaluating performance issues and concerns, and to identify productivity or related issues that need additional educational focus within the District. Users should strive to protect any assets purchased by the District with taxpayer funds.

## 7.4 No Expectation of Privacy

Although users may be expected to maintain the privacy and confidentiality of information to which they have access, they are not guaranteed personal privacy for any activity in which they engage utilizing VIFR technology assets. This includes legitimate District purposes, Minimal Personal Use, violations of acceptable use or any other use. This includes, but is not limited to, word processing documents, spreadsheets, databases, electronic and voice mail, and Internet access. Users should be aware that all activity undertaken on any VIFR asset, including legitimate District purpose, Minimal Personal Use, violations of acceptable use or any other purpose, is subject to monitoring, recording and intervention by District management for the purpose of system updates, maintenance, security and compliance with District policies and standards. Any use of VIFR assets constitutes user consent to such monitoring, recording and intervention. Users expecting privacy for their Minimal Personal Use should use a different means of communication. Users should be aware that electronic communications could be forwarded, intercepted, printed and stored by others and are not subject to personal privacy expectation. Such communications may be disclosed pursuant to public disclosure laws and rules of discovery in the event of lawsuits.

## 8.0 Policy Statement – Acceptable Use of Information Technology Assets

Users shall ensure that VIFR Information Technology Assets are used appropriately for District business. Users shall use these assets to increase

# Vashon Island Fire & Rescue Operations Manual

Policy 9001:

Acceptable Use of Information Technology

Effective Date

06/24/2014

Approved and Issued:

06/24/2014

productivity, facilitate the efficient and effective performance of their duties, and meet the daily operational and business requirements of VIFR, including but not limited to the following illustrative list, to:

- 8.1.1 Perform assigned responsibilities and duties;
- 8.1.2 Support Vashon Island Fire and Rescue activities;
- 8.1.3 Access authorized work-related information;
- 8.1.4 Communicate and collaborate with colleagues on work-related issues;
- 8.1.5 Improve work-related skills when approved by management;
- 8.1.6 Use applications and access information available on VIFR Internet and Intranet sites;
- 8.1.7 Access Internet hosted on-line reference and information sources such as phone directories, online dictionaries, search engines, subscription resources, or mapping and weather services if such use is appropriate for business use, adds value to the organization, increases employee efficiency or avoids costs that would otherwise be incurred by the District for such referenced services;
- 8.1.8 Access Internet-based training resources approved and/or provided by VIFR;
- 8.1.9 Comply with this policy, VIFR security standards, procedures and methods, and federal, state and local laws concerning computers, networks and the Code of Conduct;
- 8.1.10 Interact for personal use by employees with human resource, time accounting, compensation and employee benefits and health administration programs managed by or administered for VIFR.

## 9.0 Policy Statement – Prohibited Uses

- 9.1.1 Commercial Use – Users may not use any of the District’s technologies or resources for commercial use or personal financial gain.
- 9.1.2 Copyright violations – Any use of resources which violates copyright laws is strictly prohibited.
- 9.1.3 Solicitation – The purchase or sale of personal items via the network, Internet, e-mail or any District resource is prohibited.
- 9.1.4 Harassment – any use of District resources to harass employees, vendors, citizens or any other person is strictly prohibited.
- 9.1.5 Websites which contain sexually explicit photos or materials, promote pornography, gambling, hate crimes or violence.

# Vashon Island Fire & Rescue Operations Manual

---

Policy 9001:

## Acceptable Use of Information Technology

Effective Date  
06/24/2014

Approved and Issued:  
06/24/2014

---

- 9.1.6 Social Networking while on duty *unless such use is minimal* and not during response, duties or while undergoing training; participating in social networking from VIFR equipment or apparatus; participating in social networking while being identifiable as a spokesperson of VIFR.
- 9.1.7 Political – the District’s resources may not be used to further any political purpose or make unauthorized public statements on behalf of the District.
- 9.1.8 Any activity that could cause the loss, corruption of or prevention of rightful access to data or the degradation of the system or network performance or breach its security.
- 9.1.9 Aliases – The use of aliases to disguise one’s identity using District resources is prohibited. Anonymous messages via the Districts intranet or email system are prohibited. Misrepresentation of one’s identity, misusing another user’s account or misrepresentation of status, job title, position or level of responsibility is strictly prohibited.
- 9.1.10 Knowingly access, use, copy, modify or delete files, data, user accounts, access rights, logs, applications, system functions, drivers or disk space allocations associated with VIFR assets without proper authorization.
- 9.1.11 Misinformation/Confidential information - The release of false, distorted, misleading or confidential information is prohibited. In that medical information may be contained or transmitted on District equipment, release of confidential medical information to unauthorized persons in violation of H.I.P.A.A. is forbidden.
- 9.1.12 Any site charging a fee for non-business related usage. Business purchasing must use established purchasing policies. If you visit a site by mistake, do not give out any billing information such as credit card or business phone. If you are asked for billing information, cancel out of the screen immediately.
- 9.1.13 The use of unauthorized software on District computer systems is prohibited. Consequently, employees and volunteers shall not use the Internet to download or install unauthorized software on District computers without the permission of the Systems Administrator.
- 9.1.14 All users of the District’s technology equipment are expected to act lawfully, ethically and professionally and to exercise common sense. Actions that would be embarrassing to explain to the public or the Fire Chief should be avoided.

# Vashon Island Fire & Rescue Operations Manual

Policy 9001:

Acceptable Use of Information Technology

Effective Date

06/24/2014

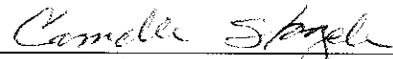
Approved and Issued:

06/24/2014

## 10.0 Policy Statement – Responsibilities

- 10.1 Users understand the expectations of this policy and accept personal responsibility for adhering to its provisions. In addition, all members are responsible to safeguard and protect District assets and reputation from anything other than authorized and intended use. The security of private, personal information of fellow co-workers as well as the confidentiality of the public we serve depends on such vigilance.
- 10.2 Supervisors should make users aware of this policy, educate them about its content and require that employees acknowledge receipt of such policy and the impacts of violating it.
- 10.3 System Administrator - In addition to assisting department/division users in the acquisition, repair and use of computer systems, the System Administrator is responsible for facilitating and monitoring compliance with this procedure.
- 10.4 Installation of Software and Hardware - All computer software and hardware shall be installed and configured by the System Administrator. Any moving, relocating, or rearranging of computer hardware shall also be coordinated with the System Administrator and with the approval of the Fire Chief or his designee.
- 10.5 Backup of Data Files - The System Administrator or assigned Administrative Assistant regularly backs up data files stored on the Local Area Network (LAN) on cassette tape in order to avoid irretrievable loss through hardware failure. These are stored off-site. This backup procedure is designed for catastrophic backup purposes only and not intended as a file retention or archive method.
- 10.6 If any computer is malfunctioning, or software, email account or cell phone is not working or the user is having difficulty logging in, the System Administrator or designee shall be contacted as soon as possible for repair.

Approved:



Board Chair of Fire Commissioners  
Vashon Island Fire & Rescue

Date:

