Northwest Workforce Council

Policy: **Acceptable Use of Communications and Computing Resources**

Number: **WIOA 01-08**

Effective: **February 10, 2017**

BACKGROUND:
Northwest Workforce Council's technical resources, including voice mail, e-mail, phone, mobile devices, internet, and computer systems are provided for use in the course of the company's business, and such use is authorized under this policy. Because their primary purpose is to facilitate communication and data regarding the company's business, these resources are neither private nor confidential. The Council has the ability and retains the right to monitor, review communications and use history, and archive at any time. Voice mail, email, text messages, Internet history and other use data may be retrieved and reviewed when necessary for business reasons or other interests of the Council. For these purposes the Council may override any applicable passwords or codes to obtain access to, or review, copy, archive, or delete, its communications, data and/or devices.

POLICY:
A. Responsibility
Management must ensure employees and business partners using or accessing the Council's computing and communications resources receive an orientation on the appropriate use of the resources. Employees represent the Council at all times when using computing and communications resources to conduct Council business.

Employees must ensure their use conforms to the limitations and parameters expressed in this policy, take reasonable caution and abide by Council procedures to prevent the theft of equipment and loss of data from Council owned devices or networks. This policy requires the use of judgement. If there is any doubt about the use of the Council's information technology resources, the employee should first check with their supervisor or the regional manager.

B. Employee Use of Electronic Messaging Systems and the Internet

1. **Permitted Business Use** – Computing and communication devices, electronic messaging systems and internet access provided by Northwest Workforce Council may only be used to conduct business reasonably related to that of the Council.

2. **Permitted Personal Use** - Council staff may make occasional, limited, personal use of Council's resources such as electronic messaging systems and the internet if the use conforms to all of the following ethical standards:
    a) There is little or no cost to the Council;
    b) The use does not interfere with the performance of the employee's duties;
    c) The use is brief in duration and frequency (e.g. able to be accomplished within a 10 minute break period. See appendix for examples). Employees are expected to exercise good judgment in both duration and frequency;

    d) The use does not disrupt or distract other employees and does not obligate them to make personal use of Council resources; and
    e) The use does not compromise the security or integrity of Council information, devices or software.

C. Prohibited Uses - Employees may never use Council provided computing and communication resources in any of the following ways:

1. To transmit unencrypted, sensitive or confidential information (including program decisions, HIPPA protected information, or other participant information or services provided) via e-mail, text messaging, or over the internet.
2. To make unlawful or inappropriate disclosures of confidential information.
3. To make personal use of Council provided devices, electronic messaging systems, networks or internet access that does not meet the conditions described above in Section B.2. a-e.
4. To derive personal benefit or financial gain.
5. To conduct activities that support or are associated in any way with outside employment.
6. To create, access, post, send or print any sexually explicit, obscene or pornographic material.
7. To connect to internet sites or create, transmit or store electronic messages that contain or promote:
    a) Discrimination on the basis of age, race, color, gender, creed, marital status, national origin, disability, religion, sexual orientation or disabled and Vietnam era veterans status;
    b) Harassment or threats;
    c) Copyright infringement or violations of software licensing agreements;
    d) Personal religious or philosophical beliefs;
    e) Political campaigns, initiatives or personal political beliefs;
    f) Personal business interests, including commercial uses such as advertising or selling; or
    g) Any activity prohibited by federal, state, local law, or Council policy.
8. In addition, employees may not use Council provided devices, networks or internet access to:
    a) Order or sell items on the internet, except as specifically approved by Council for business purposes or sponsored activity;
    b) Participate in any sponsored online game, contest, promotion, or sweepstakes for personal financial gain;
    c) Participate in non-work-related instant messaging, texting, e-mail lists, blogs or newsgroups;
    d) Gamble or participate in any related gaming activities;
    e) Solicit money for religious or political causes or for non-Council events;
    f) Create, post, transmit, connect to or voluntarily receive offensive, libelous, threatening or harassing material;

g) Spread malware, gain unauthorized access to another computer, make another network unusable by intentionally disrupting connections to prevent access to a service or “flooding” a network to prevent legitimate network traffic;

h) Conduct personal banking or financial transactions unless directly associated with the Council’s profit sharing plan or 401K retirement system; or

i) Access social media accounts for personal use.

j) Stream or download content or data from any source unrelated to official Council business.

9. Accessing personal web-based e-mail accounts or personal instant messaging services using Council computers, devices, networks and communication lines is permitted only when that use conforms to Section B. 2. of this policy.
10. Transmitting and storage of Council data or conducting Council business via personal e-mail, personal messaging applications, or personal cloud storage is strictly prohibited. Employees may not use or install e-mail, unapproved applications, or messaging software on Council computers and devices.
11. Employees must not create, forward or store electronic messages in Council locations including but not limited to, local computer storage, mobile device, and/or e-mail inbox that do not pertain to Council business. This includes, but is not limited to, hoaxes, hypes, chain letters and spamming messages to/from any computing and communications resources.
12. Employees must not use the Council’s computing and communication resources, networks, or devices to transmit, receive, play or download video or audio unless it is expressly required for work-related purposes.
13. Employees may not download software from the Internet. When there is a clear business reason for downloading Internet software or mobile device applications (apps), written approval from the Regional Manager must first be obtained.
14. Employees should not open emails or attachments from unknown, unfamiliar, or unusual sources. More detail is provided in the document, PC Security Guidance.
15. Employees may not store any customer (e.g. any business or job seeker/candidate connected to NWC for business reasons) information on portable media storage devices (flash drives, CDs, DVDs, etc.) or personal cloud-based storage.
16. Employees may not store any customer information on Council owned mobile devices such as phones or laptop computers, which do not have an encryption program activated. (Council tablets do have active encryption software.)
17. Employees may not save personal photos, videos, music, documents, or games on Council servers or devices.
18. Employees are prohibited to move, remove or configure Council owned equipment such as printers, phones, network cables, computers and other peripheral devices without first securing written approval from the Regional Manager.
19. Employees are prohibited to connect non-Council appliances to the Council’s networks such as laptops, tablets, desktops, wireless routers, printers, switches, hubs, firewalls, mobile phones or other devices.

D. Mobile Devices

1. Staff are required to produce Council-owned devices upon demand.
2. Authorized users are considered the first line of security, responsible to keep the device physically secure, either in staff's possession at all times or in a secure physical location. When the device is in transit and not on the staff's person, the device must be locked out of sight, such as a trunk or glove box.
3. Any employee who is the authorized user of a mobile device that it is lost, stolen and/or damaged and/or who suspects that data has been in any way compromised must immediately notify the regional manager.
4. Devices reported as compromised, lost or stolen will be remotely wiped clean of all data and locked out.
5. The device's data encryption must not be disabled at any time.
6. GPS or other location services are enabled at all times to help locate device if lost or stolen.
7. The use of Bluetooth is prohibited with tablet devices as the connections can be used to access sensitive data.

E. Passwords

Passwords, PIN codes, and other similar methods of securing the Council's computing and communication resources are created by the individual user. All passwords must contain at a minimum eight (8) characters with at least one (1) upper case letter and at least one (1) special character (#, &, etc.). Each site or program used by the employee conducting NWC business must have a unique password. Passwords are not duplicated or repeated for multiple sites. They shall be kept confidential and must never be shared (excepted below).

A contemporary catalogue of passwords used to conduct Council business or on Council devices is securely maintained by the regional manager for security purposes. This allows for a review of each password to verify conformity to policy and may, if needed, be used by the regional manager or designee to retrieve information.

F. Security and Virus Protection

Each NWC device is protected with security features which run constantly in the background. Each device is remotely monitored to ensure its operational health and integrity. To ensure security patches are installed in a timely manner, all employees are to leave their NWC PC, laptop, and/or tablet running, logged off, and connected to the Council's network on the weekday specified by the regional manager.

G. E-mail

It is the responsibility of all staff to ensure *Automatic Replies (Out of Office)* is used when you will not be in the office for one (1) work day or longer.

All direct service staff must follow the protocol established for e-mail signature. The protocol for e-mail signature is found on DAWN.

Do not open an attachment or click on a link received via email that you aren't expecting, regardless of the sender. If you know the sender, alert them to the received email and confirm they intended to send it before clicking a link or opening any attachments. Sometimes phishing emails contain obvious spelling and grammar errors that are easy to spot, but others can be indistinguishable from legitimate emails.

H. Voice Mail

All employees will record a personalized voice mail message/greeting that provides sufficient information for the caller to determine their next steps. Messages/greetings must be kept up to date and modified promptly to account for schedule changes, vacation leave, holidays and unplanned absences. Telephone messages will be returned by close of business the next business day. The protocol for voice mail is found on DAWN.

Violation of Policy

Violation of this policy, and/or misuse of the company's electronic and communication resources is subject to discipline, up to and including, an individual's immediate termination of employment.

Appendix 1

DEFINITIONS: Not all definitions listed below are contained in the policy. They are listed to help better understand the various complexities one may encounter as they use communication and computing resources.

Blog: A blog (a contraction of the term "web log") is a type of website, usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video.

Cloud storage: Data that is saved to an off-site storage system and is maintained by a third party. The Internet provides the connection between the user's computer and the remote storage.

Computing and communications resources: Technology products and services, including but not limited to, computers, peripherals, fax machines, electronic messaging systems, Council controlled networks, servers, telecommunications systems, wireless communications devices (such as cell phones, tablets, “Wi-Fi”, Bluetooth), including resources owned or operated by partner organizations.

Compliance Archiving: is the act of preserving and making searchable all company e-mail to/from an individual. E-mail archiving solutions capture e-mail content either directly from the e-mail application itself or during transport.

Electronic messaging system: Any electronic messaging system that transmits and/or stores voice recordings or typed communication. These messaging systems are commonly referred to as voice mail, e-mail, fax, and text messaging.

Encryption: The translation of data to make it unreadable except to those in possession of a secret key, cipher, or password.

Firewall: A system or combination of systems and software that enforces access control policies between two or more networks.

Hoaxes, **hypes**, **chain letters** and **spamming:** Terms used to describe electronic messaging that is sent to a large number of recipients or is intended to eventually spread to a large number of recipients.

Instant messaging: A type of communications service that enables a person to engage in instantaneous direct person to person communication with another individual or individuals. Instant messaging includes, but is not limited to, internet based chat and online messaging services such as Google Talk.

Malware: Short for malicious software, software designed specifically to damage, disrupt or cause a system to perform in a way other than its designed purpose, such as a virus, worm, spyware or Trojan horse.

Mobile device: any portable communication or information gathering device used to access, store, or manipulate data, e.g., smartphone, tablet, laptop or notebook computer.

Network: An interconnected group of computers which allow users to share resources and communicate.

Newsgroup: An online discussion group that communicates about a particular subject with notes written to a central internet site and redistributed through Usenet, a worldwide network of news discussion groups.

Phishing: A method of obtaining information such as passwords, usernames, and credit card details by posing as trustworthy services or known persons.

Social Engineering: The art of manipulating people into performing actions or divulging confidential information. This is a type of confidence trick for the purpose of information gathering, fraud, or computer system access

Social media: Refers to interactive web-based technologies used for social networking and for sharing, discussing, and/or developing content. Types of social media include, but are not limited to, blogs, video- or photo-sharing sites, and social networking sites. Examples of social media sites include YouTube, Twitter and Facebook.

Social networking: Refers to the use of social media for connecting with others and/or building online communities.

Streaming video or **audio**: Streaming is the process of moving images or sounds in a continuous stream over the internet in compressed format to be displayed or played when they arrive. With streaming, a web user does not have to wait to download a large file before seeing the video or hearing the sound. The user needs a player, which is a special program that decompresses and sends video data to the display and audio data to the speakers.

Appendix 2

Illustrative Examples of Permitted and Prohibited Use

Example 1: An employee makes a local telephone call or sends an e-mail communication to their home to make sure their children have arrived safely home from school. This is not a violation of this policy. There is no cost to the Council and because the call or e-mail is brief in duration, it does not interfere with the performance of job duties.

Example 2: An employee uses their computer to send electronic mail to another employee regarding the agenda for a workgroup meeting that both will attend. He also wishes the other employee a happy birthday. This informal personal message is brief. There is no violation of policy in this example.

Example 3: Several times a month an employee quickly uses the internet to check his children's school web site to confirm if the school will end early that day. The inquiry takes about five minutes. This is not a policy violation. The use is brief and infrequent, there is little or no cost to the Council, and the use does not interfere with the performance of the employee's job duties.

Example 4*: An employee routinely uses the internet to manage their personal investment portfolio and communicate information to their broker. This is a violation of this policy. Using Council resources to routinely monitor private stock investments, make stock trades or to conduct personal banking or other financial transaction including those that can result in a private financial benefit or gain, is prohibited.*

Example 5*: An employee spends thirty minutes or more looking at various web sites related to a candidate for office the employee endorses. This is a dual violation of this policy. The use is not brief (up to 10 minutes) and interferes with the performance of job duties. Additionally the content of the web site is prohibited by this policy.*

Example 6*: An employee visits several humor and joke sites. While at the site, s/he downloads a joke file and e-mails it to several coworkers. This is a violation of this policy. By e-mailing a file to coworkers, the employee disrupts other employees and compels them to make personal use of Council resources. In addition, downloading files and distributing them to coworkers can introduce a computer virus or malware.*