# 4.08 INFORMATION TECHNOLOGIES

**Purpose**

The City of Portland provides information technologies to Authorized Users, including its employees, to use in the course of conducting City business. This administrative rule covers the use of City Information Technologies for internal and external communication and as a research tool and information resource.

This administrative rule mandates ethical use of City Information Technologies, encourages use that supports productivity, confirms that electronic communications created and used for conducting City business are generally considered public records, and prohibits inappropriate use.

The Bureau of Technology Services (BTS) maintains authority for the technical rules and standards of City Information Technologies and the Bureau of Human Resources (BHR) maintains authority over employee behavior in the use of those technologies. All Authorized Users of City Information Technologies are responsible for reading and complying with this administrative rule.

**Definitions**

**Authorized User:** Any person employed, volunteering or working on behalf of the City, its Bureaus, Divisions, Offices and Directors; and any person or entity contracted or authorized to use City resources in the course of providing goods and services to the City.

**City Information Technologies:** Includes, but is not limited to, authorized computer and telecommunications hardware, software, cloud and web services, and systems that utilize the internet and/or any other communications network.

**Authorized Use of City Information Technologies**

**Use for City Business:** Authorized Users must only use City Information Technologies for professional business use in performing job-related, or otherwise authorized, City duties or functions.

**Security and Integrity of City Information Technology:** Authorized Users must protect the security, Confidentiality and integrity of City data, equipment, and technology assets and of City employees, contractors and customers. See HR Administrative Rule 11.04 Protection of Restricted and Confidential Information.

**No Expectation of Privacy:** Authorized Users have no expectation of privacy in the use of City Information Technologies. All use of City Information Technologies, and any information created or stored by Authorized Users on City Information Technologies, are City property, subject to public records requirements and City monitoring and reporting.

**Compliance with Laws and Regulations:** Use of City Information Technologies must comply with all applicable federal laws, Oregon Revised Statutes, City Code and City Administrative Rule provisions, and any bureau-specific work rules. Authorized Users must comply with all accepted standards and practices for use.

When conducting City business, employees, City Elected Officials and all other Authorized Users should always use City email and authorized City Information Technologies.

**Use for City Business**

**Authorized Users must only use City Information Technologies for professional business use in performing job-related, or otherwise authorized, City duties or functions.**

Authorized Users are required to ensure their use of City Information Technologies is limited to authorized purposes. "Use" includes:

- Use of City computers, tablets, mobile and other devices or hardware;
- Communication via email, text messages, instant messaging, social media and any other communication method using City Information Technologies (see HRAR 4.08(A) Social Media);
- Accessing the internet using City Information Technologies;
- Use of authorized cloud and web services;
- Use of City software, networks, accounts, data storage systems or information stored on any of these systems.

Acceptable uses of City Information Technologies include:

- Professional business use for job-related duties;
- Communication with other federal, state or local government agencies, their committees, boards and commissions;
- Communication for the purpose of information exchange, research, professional development or to maintain job knowledge or skills;
- Communication, information exchange and record keeping directly relating to the mission and Charter of the City of Portland and the work tasks of individual bureaus in support of work-related functions.

Authorized Users are prohibited from:

- Using City Information Technologies for **personal use or gain** not expressly allowed, such as:
    1. Buying, selling, or trading goods, services or financial instruments via the City's Information Technologies for personal financial gain.

2. Using City Information Technologies to avoid the expense of personally purchasing comparable hardware, software, and/or internet access.

3. Copying and/or using City data, regardless of physical or electronic form or media, for personal use, except as permitted by law.

- Using City Information Technologies for **political activity** or in a manner that would directly or indirectly assist a campaign for election of any person to any office, or for the promotion of or opposition to any ballot proposition. This prohibition shall not apply to the use of City Information Technologies for the development or delivery of a neutral and objective presentation of facts relevant to a ballot proposition as allowed by state law, provided that such use must be a part of the normal and regular conduct of the employees developing or delivering the presentation of facts.
- Using City Information Technologies for **commercial purposes**. City Information Technologies may not be used for commercial activities or in a manner that would constitute an endorsement of a specific commercial entity, its products, services, or business practices. An exception may be permitted if such information is central to a bureau's mission and meets stated Council goals and objectives. The exception must be pre-approved by the Commissioner in Charge or their delegate. Authorized employee discounts may be distributed with authorization from the Commissioner in Charge or Bureau Directors.
- Using City Information Technologies for **religious causes**.

**Security and Integrity of City Information Technology**

**Authorized Users must protect the security, Confidentiality and integrity of City data, equipment, and technology assets and of City employees, contractors and customers.**

Authorized Users are required to:

- Select, use and secure strong individual passwords or two-factor authentication, when available, for access to City Information Technologies (e.g. for network login, email, desktop computer, laptop, mobile device or smartphone) and never share access to accounts, privileges and associated passwords;
- Accept accountability for all activities associated with the use of their user accounts and related access privileges. Each Authorized User is responsible for their own use of a shared device;
- Ensure restricted and Confidential information about City employees, vendors, and/or the public is protected. See HRAR 11.04 Protection of Restricted and Confidential Information;
- Report all suspected security and/or policy violations to an appropriate authority (e.g. manager, supervisor, bureau director, BTS Helpdesk, Chief Information Security Officer);

- Take all malware warnings seriously and comply with procedures for reporting and responding to malware outbreaks;
- Use their real name and/or email address in all emails, news posts or any other form of electronic communication.

Authorized Users are prohibited from:

- Removing City owned information technology devices or equipment from City premises, except as specifically allowed by the User's bureau, such as taking home a City owned laptop computer for City business;
- Modifying City Information Technologies beyond normal parameters of use;
- Altering City owned or licensed software without appropriate written authorization from the Bureau of Technology Services;
- Purchasing, installing or using any software or applications not previously approved by the Bureau of Technology Services including unlicensed, free, or internet-based (cloud) service software. This does not include downloading and installing properly licensed and approved software from BTS maintained systems or as permitted by contract;
- Using software that allows a workstation or other City of Portland information resource to function in an unauthorized manner;
- Deliberately transmitting data containing malware or willfully circumventing malware protection measures;
- Misusing service or taking any action that renders the Authorized User's computer equipment unusable, or that interferes with another Authorized User's use of City Information Technologies;
- Granting or allowing access by any person or entity to City Information Technologies or data, regardless of physical or electronic form or media, for which they are not authorized to do so, such as sharing passwords with unlicensed users;
- Failing to appropriately limit the number of recipients of messages, propagating virus hoaxes, "spamming" (spreading email or postings widely and without good purpose), or "bombing" (flooding an individual or group with numerous or large -mail messages). Employees and other Authorized Users may not use the City's email to send email messages to fifty (50) or more City employees outside the sender's bureau without Bureau Director approval. Employees must obtain BTS authorization to email all City employees. See Attachment A, Guidance and Procedures;
- Altering electronic communications to hide one's identity or to impersonate another individual;
- Causing a breach of security or any action to attempt to circumvent or reduce the security of the City's computer and network resources or of any Confidential or Restricted Information, regardless of physical or electronic form or media, entrusted to the City's custody.

**No Expectation of Privacy in the Use of Information Technology**

**Authorized Users shall have no expectation of privacy in the use of City Information Technologies.**

All use of City Information Technologies and any information or data created or stored by Authorized Users on City Information Technologies are City property, subject to public records requirements and City monitoring and reporting. With few exceptions, any electronically stored information, regardless of electronic form or media, that pertains to City policies, decisions, transactions and activities is subject to public disclosure and records retention and preservation requirements. See HRAR 1.03 Public Records Information, Access and Retention.

**Passwords are required to protect the security and Confidentiality of City Information Technologies and the information they contain and are not intended to convey an expectation of personal privacy or exclusion from monitoring.**

The City Attorney or designee may access electronic information to comply with legal requirements and processes such as, but not limited to, public record requests, subpoenas, legal holds, and the electronic discovery of records for actual or potential litigation in which the City is an affected party. The City Attorney's or designee's access to records is not considered "monitoring" under these rules.

Authorized Users are required to:

- Preserve documents, emails and other electronic records created using the City's Information Technologies as public records in compliance with City record retention and preservation policies. Such records may be subject to disclosure;
- Consent to monitoring of their use of City Information Technologies, including email, text messages, social media content and logs, website visits, other transmissions and any stored information created or received via the City's Information Technologies (see Attachment A, Guidance and Procedures).

Authorized Users are prohibited from:

- Destroying City records in violation of retention and preservation policies.

**Compliance with Laws and Regulations**

**Authorized Users must comply with all applicable State and Federal Laws, Oregon Revised Statutes, City Code and City Administrative Rule provisions, and any bureau-specific work rules.**

Authorized Users are required to:

- Support compliance with all federal, state, and local statutes and regulations and applicable industry requirements;
- Comply with accepted standards and practices for use;

- Follow all applicable BTS Administrative Rules, and all specific policies, guidelines and procedures established by individual bureaus and offices as well as agencies with which they are associated and that have provided them access privileges;
- Comply with all service and contractual agreements, intellectual property rights, copyright and software license agreements.

Authorized Users are prohibited from:

- Using any City Information Technologies to commit an illegal act;
- Accessing racist, hate groups, and sexually explicit sites;
- Accessing or transmitting information that conflicts with City Code, Administrative Rules or bureau work rules for non-job-related reasons such as information in violation of the City's non-discrimination policy.

**Personal Use of City Information Technologies**

Where possible, personal use should be conducted via a personal device. However, limited personal use is permitted if:

1. It is not prohibited by law or bureau specific work rules;
2. It is incidental, occasional and of short duration;
3. It is done on the Authorized User's personal time. Personal time means during breaks, lunch and/or before and after work as defined by collective bargaining agreements, City Administrative Rules and bureau work rules.
4. It does not interfere with any Authorized User's job activities, including activities which might pose a conflict of interest or give the appearance of impropriety with an individual's employment with the City;
5. It does not result in an expense to the City;
6. It does not solicit for or promote commercial ventures, religious or political causes, outside organizations or other non-job-related solicitations;
7. It does not violate any "Prohibited Uses" section in this administrative rule;
8. It does not disrupt the Bureau of Technology Services' ability to provide information technology services to City users;
9. It meets all requirements of this rule.

An Authorized User's personal use of City Information Technologies can be denied by their bureau director due to operational or other concerns.

**Bureau Rules May Be More Restrictive**

The standards and guidelines outlined in this administrative rule are minimum standards for City bureaus and offices. Bureaus may develop rules regarding bureau-specific use of City Information Technologies, which may include more restrictive work rules based on the operational needs of the particular bureau or office, upon review and approval by BTS. All drafts of bureau-specific IT work rules must be

| | |
|---|---|
| | forwarded to the BTS Chief Technology Officer (CTO) for final approval prior to implementation. |
| **Monitoring and Reporting of Information Technologies' Usage** | The City of Portland monitors the use of City Information Technologies including email, website visits, other computer transmissions and any stored information created or received by City employees and other Authorized Users with City Information Technologies. Monitoring may result in reports logging usage and printed or electronic copies of email or stored information.<br><br>Use of the City's Information Technologies constitutes an express consent to monitoring at all times. See Attachment A, Procedures and Guidance. |
| **Union Use of City Information Technologies** | Union use of City Information Technologies is permitted in accordance with Authorized Use of City Information Technologies provided such use meets all requirements of this Rule. |
| **Technology Rules and Standards** | For Technology Services Administrative Rules, go to<br>https://www.portlandoregon.gov/citycode/index.cfm?&c=26821<br><br>For Technical Standards, go to<br>http://www.portlandoregon.gov/bts/46940 |
| **Contact Information** | Technical questions regarding the use of City Information Technologies should be directed to the Bureau of Technology Services. Any human resources related issues should be directed to the Bureau of Human Resources HR Business Partner. |
| **Administrative Rule History** | Adopted by Council March 6, 2002, Ordinance No. 176302<br>Effective April 5, 2002<br>Revised October 15, 2002<br>Revised July 28, 2003<br>Revised July 1, 2004<br>Revised January 25, 2006<br>Revised July 9, 2007<br>Revised September 28, 2009<br>Revised October 19, 2010<br>Revised November 4, 2011<br>Revised December 4, 2013<br>Revised April 25, 2016<br>Revised February 15, 2018 |

# HR Administrative Rule 4.08 Information Technologies
# Attachment A
# Procedures and Guidance

## 1. Procedures for Broadcast or "All Employee" Email Messages

Employees must first obtain Bureau Director approval to use the City's email system to send "broadcast" email messages. In this instance "broadcast" means sending an email message to fifty (50) or more City employees outside of the sender's bureau.

To send a broadcast email to City employees, the sender must follow procedures established by BTS for "All City Employees" email messages, including but not limited to including the following warning: "Please do not use the Reply to All function to respond to this message. The appropriate contact person is listed in the message." The sender must contact the BTS HelpDesk for authorization to use the "All City Employees" distribution list. Broadcast messages will be reviewed for file size.

The City's internet web page may be the most appropriate place for announcements of general interest in lieu of broadcast email messages.

## 2. Guidance for Monitoring and Reporting of Information Technologies' Usage

The City of Portland monitors the use of City Information Technologies including email, website visits, texts, instant messages, other computer transmissions and any stored information created or received by Authorized Users with City Information Technologies. Monitoring may result in reports, logs of usage and printed or electronic copies of email or stored information.

Requests for monitoring and reporting of City Information Technology use, including but not limited to the internet activity, email use and/or other communications of an individual employee or department, and/or monitoring and reporting of video/audio recording of an employee must be submitted in writing to the Director of Human Resources or designee and must be submitted by a bureau director or a city attorney. Nothing in this section requires the Director of Human Resource's approval for routine monitoring of telephone calls and other activities for quality control purposes.

Generating Reports – When the Director of Human Resources approves a monitoring request, a written request defining the desired information will be submitted to a designated Bureau of Technology Services (BTS) staff member. BTS will generate a report and submit it to the Director of Human Resources or their delegate. The Bureau of Human Resources and BTS will maintain a record of all requested reports.

- Individual Reports – Requests for monitoring a specific employee's technology use should contain a reason for the request.

- Group Reports – Requests for aggregate reports for group or bureau-wide technology use do not require a specific rationale.

Neither individuals nor groups need to be notified of monitoring. Should the report indicate use of City Information Technologies which violates bureau or City Administrative Rules, all

applicable requirements in a collective bargaining agreement or in the administrative rules must be followed prior to implementing discipline.

Confidentiality – Reports on an individual's technology usage are considered personnel information and should be treated as confidential. Electronic content may also be confidential for other reasons and will be reviewed in a manner to protect that confidentiality and to comply with all applicable laws and City rules. However, these reports are public records and may be subject to disclosure. All requests for disclosure should be referred to the City Attorney for response.

**3. Procedures for Website Blocking**

The City makes an effort to block access to certain internet content deemed by the Bureau of Technology Services Information Security Manager to be of high risk to the City network and users. This content typically has the potential to deliver malware to the City's network and/or its users or has been deemed inappropriate. Decisions to block inappropriate content will be made in consultation with the Director of Human Resources.

The Bureau of Human Resources acknowledges that on occasion, there may be a legitimate and compelling City business reason for an individual or a specific work group to gain access to internet content that is otherwise blocked. If such a situation arises, the bureau director must submit a written request to the Director of Human Resources which includes:

1. The name and position of the employee(s) for whom an exception is being requested;
2. The specific web site, category of sites, to which the employee(s) require access; and
3. The compelling City business need for access to the content.

The Bureau of Human Resources will review the request and provide a written response. The Bureau of Human Resources is predisposed to maintaining a consistent policy on internet access and may suggest alternative approaches for meeting the business need. The Bureau of Human Resources will work with the Bureau of Technology Services to determine if such a request is technically feasible. If the request is technically feasible and an exception is granted, Human Resources will send authorization and written instructions to a designated Bureau of Technology Services staff member requesting that the exception be implemented.

**4. Electronic Records Retention and Preservation**

With few exceptions, any electronically stored information, regardless of electronic form or media that pertains to City policies, decisions, transactions and activities is subject to public disclosure and record retention and preservation requirements.

- Transitory records are records of short-term interest (90 days or less), which have minimal or no documentary or evidential value. Examples are:
    1. Routine requests for information or publications and copies of replies which require no administrative action, no policy decision, and no special compilation or research for reply
    2. Originating office copies of letters of transmittal that do not add any information to that contained in the transmitted material

3. Quasi-official notices including memoranda and other records that do not serve as the basis of official actions, such as notices of office parties, holidays or charity fund appeals, and other similar records
4. Records documenting routine activities containing no substantive information, such as routine notifications of meetings, scheduling of work related trips and visits, and other scheduling related activities
5. Listserv messages
6. Fax confirmations
7. Reading materials
8. Reference materials
9. FYI email information that does not elicit a response
10. Unsolicited advertising

Emails that fall under the Transitory category should be deleted from the email system by the user as soon as any operation or informational value has expired.

Note: Calendars for elected officials and bureau heads must be retained permanently and calendars for other city employees must be retained for one (1) year.

- Correspondence are records that directly relate to City programs, management or administration. These include but are not limited to formal approvals, directions for action, communications about contracts, purchases, grants, personnel, etc.; and correspondence relating to a particular project or program.

Records that fall under the Correspondence category must be managed as an official City record in a suitable storage environment. See HRAR 1.03 Public Records Information, Access and Retention.