CITY OF RICHARDSON

INTERDEPARTMENTAL POLICY AND PROCEDURES

ELECTRONIC COMMUNICATIONS AND TECHNOLOGY RESOURCES

1. **Purpose**

1.1. This Policy governs the use of the Technology resources owned and operated by the City of Richardson Texas by employees, volunteers, vendors, contractors and all other authorized users. Technology includes, but is not limited to, desktops, laptops, mobile devices, networking equipment, networked devices, servers, software, electronic mail, phones, cellular phones, control systems, Internet, Intranet, radio signaling devices, and all other Enterprise electronic systems or devices.

1.2. This policy shall apply to all City employees, volunteers, vendors, contractors, and other authorized users as defined herein.

2. **Definitions**

2.1. For the purposes of this Policy and Procedure, the following definitions shall apply:

2.1.1. Improper Material - Pictures, posters, calendars, graffiti, objects, promotional materials, reading materials, or other materials that are racist, sexually suggestive, sexually/racially demeaning, pornographic, offensive, intimidating, harassing, disparaging, and/or hostile on the basis of age, disability, gender, national origin, race, color, religion, or any other legally protected characteristic. Bringing any such material into the work environment, or possessing it to read, display, or view at work, or otherwise publicizing such materials in the work environment is specifically prohibited.

2.1.2. Chief Information Officer/CIO - The Director of Information Technology of the City of Richardson or designee.

2.1.3. Department Head - The head of an administrative department of the City of Richardson, Texas, or designee.

2.1.4. Employee - For the purpose of this policy, an employee is defined as an individual employed by the City on a full-time, part-time, or internship basis.

2.1.5. Mobile Device – Means a device intended to be portable, carried on one's person, or readily moved from location to location, such as smartphones, cell phones, radios, pagers, laptops, tablets, and others.

2.1.6. Authorized user – An authorized user is a current employee, contractor, vendor, or other party who has been granted lawful access by the Chief Information Officer to the City of Richardson network, applications, or services.

3. **Policy**

3.1. The City electronic communications and technology resources are provided for the purpose of conducting City business. City officers and employees are obligated to conserve and protect City electronic communication and technology

resources for the benefit of the public interest. Responsibility and accountability for the appropriate use of City electronic communication and technology resources ultimately rest with the individual City officer or employee or with the City officer or employee who authorizes such use.

3.2. Improper use of the City's electronic communications and technology resources may result in disciplinary procedures, up to and including termination.

3.3. City electronic communications and technology resources include, but are not limited to, computer systems, Telecommunications systems, networks, supporting equipment, and services such as e-mail, telephones, cell phones, voice mail, data storage, and Internet use.

3.4. The Information Technology Department shall establish and maintain specific rules and requirements relating to the safe and secure operation of all devices and the storage of data while connected to City resources. Adherence to these standards is a requirement for all persons utilizing city-owned devices, or storing and accessing data on city technology infrastructure. These standards shall be amended as necessary to remain current with various needs and risks, and are included in this policy by reference. Failure to comply with these rules and requirements shall be considered an improper use.

4. PROCEDURES

4.1. Appropriate Use

4.1.1. Privacy - No authorized user accessing or using computers or telecommunications resources owned and/or operated by the City of Richardson can have any expectation of privacy in the use of those resources regardless of the nature of said use. The City of Richardson reserves the right to monitor, intercept, archive, view, or distribute any and all communications and/or content transmitted over any telecommunications facility or computer resource which it owns, leases, or operates, at any time, and for any reason, without notice of any kind whatsoever to any person accessing such resources, regardless of the source or destination of said communication, subject to all applicable laws.

4.1.1.1. Information Technology Staff charged with the operation and maintenance of the City’s computers and telecommunications infrastructure may, from time to time, be required to access any and all material currently located on those resources.

4.1.1.2. Department Heads may monitor employee use of the Internet and email, and may revoke an employee’s access to the Internet and/or email by notifying the Chief Information Officer.

4.1.1.3. Authorized users must, at all times, be aware that **any** digital record residing on a city-owned device may be subject to lawful open records requests. In addition, any data regarding City business stored on a personal device or file sharing service is also subject to lawful open records requests.

4.1.1.4. The department to whom an electronic device has been issued is responsible for all costs associated with the damage or loss of any device which has been issued by the Information Technology department to one of the department's employees.

4.1.2. Resource Access Requirements

4.1.2.1. Work Product

4.1.2.1.1. Without specific authorization, no employee shall read, alter, delete or provide copies to any third party, of any digital work product created or developed by any employee or contractor of the City of Richardson .

4.1.2.1.2. No employee shall use the Internet or e-mail to present his or her own personal views, ideas, questions, or actions, as representing the positions or policies of the City unless doing so in an official capacity and authorized by the City Manager or his/her designee.

4.1.2.1.3. Unless otherwise specified by contract, any work produced by a vendor, contractor, or other third party acting as an agent, consultant, or contractor to the City, is the property of the City, and employees shall take steps to ensure that such property is properly stored on City resources to prevent loss.

4.1.2.1.4. No employee shall use any City-owned equipment or resources in violation of any applicable law.

4.1.2.2. Identity - Each person authorized to access the City of Richardson's computer and network resources must do so using a unique user name (login name) assigned by the IT Department. The use of group accounts will be limited to only those circumstances approved by the Chief Information Officer. Employees shall not share their account information, or permit other employees to log in using their credentials excepting properly identified members of the Information Technology department. Electronic communications authored by the employee must clearly originate from the user's unique account.

4.1.2.3. New Employees

4.1.2.3.1. It is the responsibility of each Department Head to notify the Information Technology Department at least three working days prior to the start date of any new employee or authorized user who

needs access to the City's electronic resources, so that appropriate access can be provided on a timely basis.

4.1.2.3.2. New employees must receive a copy of this policy, and acknowledge that they have read, and will adhere to, the contents of this document.

4.1.2.3.3. It is the responsibility of each Department Head to immediately notify the Information Technology Department in the event of the termination, resignation, or retirement of any employee within their department who previously had access to City computers and/or network resources, so that such employee user accounts may be removed.

4.1.2.4. Internet - It is the policy of the City of Richardson to offer connectivity to the Internet for employees requiring its use as a part of their normally assigned duties. The purpose of this policy is not to discourage the use of the Internet, but to provide a uniform approach to the usage of this resource, to safeguard city interests in the use of the Internet, to meet all applicable laws, to insure that all documents related to the City of Richardson that are published on the Internet conform to City standards, and to protect the assets attached to city networks from unauthorized access. The City of Richardson reserves the right to monitor all Internet usage on City-owned and City-connected computers including reviewing all sites that are viewed by the employee's browser and the amount of time spent at each site.

4.1.2.4.1. Appropriate Uses of Internet Resources - All City-owned Internet resources are to be used only in the pursuit of appropriate city business interests.

4.1.2.4.2. Bringing improper material into the work environment or workplace, or possessing any improper material at work to read, display, or view at work, or otherwise publicizing it in the work environment is prohibited.

4.1.2.4.3. No employee shall connect to any web site that contains improper material (Exception: sanctioned RPD employees performing assigned investigative work). The city reserves the right to block employee access to such web sites. Creating, sending, and/or printing Internet and/or e-mail messages which contain improper material is prohibited.

4.1.2.4.4. No employee shall operate or advertise any non-city business on the Internet using City equipment at any time.

4.1.2.4.5. No employee shall send chain letters, pyramid schemes, or unsolicited bulk email using City equipment at any time.

4.1.2.4.6. No employee shall use official City email addresses to distribute jokes, virus warnings, sentimental missives, rumors, political commentary, or other non-work-related material to other employees or the general public. (NOTE: Only Information

Technology employees, acting in their official capacity, are to transmit virus warnings.)

4.1.2.4.7. Employees shall not engage in, or advertise, any activity in which they have a personal financial interest ("moonlighting") using any City-owned electronic asset or service.

4.1.2.4.8. Personal email messages or other non-city related usage of Internet resources should be held to a minimum, as with telephone calls. Personal Internet usage or usage of electronic devices should not impede the conduct of City business; only incidental amounts of employee time - comparable to reasonable coffee breaks during the day - should be used to attend to personal matters. Questions regarding the extent of this policy should be discussed with departmental supervisors. Personal use of Internet resources is a privilege, not a right. As such, the privilege may be revoked at any time and for any reason. Abuse of the privilege may result in appropriate disciplinary action.

4.1.2.4.9. All employees shall use only their city-assigned email address during the performance of their assigned job duties. No private or "ghost" accounts shall be used, except by network administrators as part of their function (e.g., account names like "Webmaster", "Postmaster", "root", etc.) and special investigations. All requests for exceptions to this policy must be approved by the Chief Information Officer.

4.1.2.4.10. Email received from citizens should be handled with the same seriousness as any other form of citizen contact. Employees should always maintain professional decorum in their responses, seek approval from supervisors where appropriate, and reply to messages promptly.

4.1.2.4.11. Unless specifically approved by the Chief Information Officer, all Internet email transmissions shall be routed though the official city gateway service (Exception: sanctioned RPD employees performing assigned investigation work). No department or employees shall operate within city networks any email servers, mail forwarding services, or other email transmission or reception services for use by any person or automated system.

4.1.2.4.12. Internet traffic will be filtered to prevent access to inappropriate sites and those deemed detrimental to network services.

4.1.2.5. INTERNET PUBLICATION - Unless specifically approved by the Chief Information Officer, all public web documents related to the City of Richardson shall be published on the appropriate city-owned web sites or on selected social media sites when authorized by the Director of Communications and/or designee. All documents therein shall be considered official publications of the City of Richardson.

4.1.2.5.1. No department or employee shall operate any web server or other service intended to offer documents, images, or other data directly to the general public, on any city network without prior written approval from the Chief Information Officer.

4.1.2.5.2. It shall be the responsibility of the Director of Communications and the appropriate Department Head to determine that any content proposed for publication is appropriate and meets City standards.

4.1.2.5.3. Employees shall not publish on any Internet information server other than those operated by the City of Richardson, information or opinions pertaining to the City of Richardson, its operation, or their employment with the City.

4.1.2.5.4. No department or employee shall operate a network service intended for internal employee-only use (Intranet) without prior specific written approval of the Chief Information Officer. Departments wishing to publish "internal circulation only" documents shall use the server located at www.cor.gov.

4.1.2.5.5. Employees shall not place links on any City web site page that point or connect to any entity in which they have any financial interest.

4.1.2.5.6. Employees shall not engage in political activity (except when acting on behalf of the City, e.g., while conducting authorized lobbying as a representative of the City), or promote any commercial service or product, using City Internet resources.

4.1.2.5.7. Employees shall not take actions which have the effect of circumventing any filtering technology, firewall, monitor, or other application designed to limit usage of telecommunications resources.

4.1.2.5.8. Employees are not permitted to represent the City on social media sites unless explicitly authorized by their Department Head to do so.

4.1.2.6. Remote Access to Resources – The City maintains various systems to permit users to access internal systems from non-secured locations, like the Internet. These services are intended to augment the productivity of Employees.

4.1.2.6.1. Non-Exempt employees must obtain written permission from their department head to access remote access resources, including, but not limited to, email gateways, VPN servers, and file services.

4.1.2.6.2. Employees must take extra precautions when accessing City resources from non-city devices. The use of an IT-approved virus scanner is required.

4.1.2.6.3. It is the responsibility of the employee using the remote access facility, to ensure that unauthorized persons cannot utilize their account to gain access to City resources. Employees are

cautioned not to provide their passwords to anyone, including family members.

4.1.2.6.4. Users must understand that attaching their personal device or computer to City resources may impose a possibility of open records access responsibility.

4.1.2.7. Third Party Hosting and File Transfer (cloud) Services

4.1.2.7.1. Employees shall not use their personal file storage or transfer accounts (example Dropbox or iCloud) to host or store City Documents or work products unless allowed per section 4.1.2.7.2.

4.1.2.7.2. Employees needing access to third party services must:

4.1.2.7.2.1. Obtain the permission of their Department Head and;

4.1.2.7.2.2. Obtain the approval of the Chief Information Officer and;

4.1.2.7.2.3. Submit all account names and passwords to the Information Technology department to prevent data loss or security breach.

4.1.2.7.3. Employees are not permitted to conduct business on behalf of the City of Richardson using any third party email service unless allowed per section 4.1.2.7.2.

4.1.2.8. Personal Device Usage

4.1.2.8.1. The City of Richardson reserves the right to disconnect, or prevent connection to City network resources of any device, by any user, at any time, or for any reason, without any notice whatsoever.

4.1.2.8.2. The employee attaching their personal device to a City network resource assumes full liability for any risks, including, but not limited to, partial or complete data loss, errors, bugs, hardware loss or damage, viruses, malware, or any other issue which may damage the device, in any way whatsoever. The employee assumes all risk by connecting to the resource.

4.1.2.8.3. Employees shall not attach any form of network equipment, including, but not limited to, switches, routers, modems, hotspots, or any other device intended to be an intermediary data transport, to any City network, without exception.

4.1.2.8.4. The Chief Information Officer, or designee, shall be solely responsible for determining which devices may be connected to City resources. Employees should contact the Information Technology Help Desk to determine whether their device is eligible, and to obtain proper user credentials for their device.

4.1.2.8.5. **Support** – The Information Technology department will provide support for network connectivity issues. However, hardware and software support for personal devices will not be provided.

4.1.2.8.6. Reimbursement – Connection to City-owned network resources is provided to employees as a convenience only. The City will not reimburse any expense, partial or otherwise, for any usage of a personal device, including cell phones, regardless of purpose. Unless specifically authorized in writing by their department head, non-exempt employees may not use electronic devices to conduct City business outside their normal working hours.

4.1.2.8.7. Personal Device Security

4.1.2.8.7.1. In order to prevent unauthorized access to City resources, personal devices must be password protected with a strong password or keycode. Access to City resources will be denied if this protection is disabled or not present.

4.1.2.8.7.2. Employees that have been issued a City owned cell phone for their use shall not forward calls to any personally owned device.

4.1.2.8.7.3. Rooted or “jailbroken” devices will not be permitted to connect.

4.1.2.8.7.4. Users of personal devices must follow all City policies with respect to acceptable use while attached to City network resources.

4.1.2.8.7.5. Employees must be aware, that the conduct of City business, or use of City data on any personally owned device, may expose that device and the employee to legal obligations with respect to municipal open records requirements.

4.1.2.8.7.6. The employee agrees to enroll into the City’s Mobile Device Management (MDM) system. This will connect email, calendar and contacts and will also allow the City to set and enforce provisions of this policy.

4.1.2.8.7.7. The Employee is responsible to ascertain if, in the event of a remote wipe, the personal smart device allows only the City data to be erased or if personal data is vulnerable. The City recommends that the Employee take additional security precautions and the City will not be responsible for loss of personal data in any event.

4.1.2.8.7.8. Smartphones and tablets belonging to employees that are for personal use only, are not allowed to connect to the network unless given an exception in writing by their Department Head and the Chief Information officer or designee.

4.1.2.8.7.9. Employees are not automatically prevented from downloading, installing and using any app that does not appear on the list of approved apps, but may be asked to remove apps that have the potential for creating a risk for which the City would become liable.

4.1.2.8.7.10. The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) Information Technology detects a data or policy breach, a virus or similar threat to the security of the city's data and technology infrastructure.

4.1.2.8.7.11. The employee is responsible for backing up all data on their device.

4.1.2.9. Mobile Device Safety - All City employees are expected to drive with safety as the first consideration. This includes driving safely while operating cellular telephones, electronic paging devices, and/or other wireless communications devices. Recommendations for safe handling of vehicle-based calling from the wireless communications industry include the following:

4.1.2.9.1. Employees should exit the roadway to a safe area if they need to use an electronic device, and take all precautions to ensure that they do not allow the use of an electronic device to create any unsafe condition.

4.1.2.9.2. Employees are responsible for, and will be held accountable for, safe driving at all times.

4.1.2.9.3. Remember that both the City <u>and</u> the employee can be subject to liability for accidents caused by insufficient attention when driving while conducting City business (either in City–owned or personal vehicles). Employees are subject to the laws of any local jurisdiction in which they are performing their job duties, while utilizing any mobile device.

4.1.2.10. Communications Network

4.1.2.10.1. No employee or other person shall install or move any network device onto the City communications network under any circumstances whatsoever. Only members of the Information Technology department are permitted access to such equipment.

4.1.2.10.2. No employee, contractor, or third party may install any device or software intended to monitor, capture, or eavesdrop upon, any portion of data traversing the City Network, excepting members of the Information Technology department acting in the performance of their assigned duties.

4.1.2.10.3. No employee will permit any third party to connect any device to any Ethernet jack or wireless service without the express permission of the Chief Information Officer or designee, unless service is specifically provided for such purpose.

4.1.2.10.4. No employee shall install, or operate any equipment or service which has the effect of redirecting or proxying any network traffic to or from any other network, or disguising the source of any network transmission.

4.1.2.11. Software

4.1.2.11.1. The City is committed to preventing copyright infringement. It is the policy of the City of Richardson to respect all computer software copyrights and to adhere to the terms of all software licenses to which the City is a party. The City is subject to all copyright laws pertaining to the use of copyrighted software and documentation. Unless expressly authorized by the software licensor/developer, the City of Richardson has no right to make copies of the software except for backup or archival purposes.

4.1.2.11.2. All software used on a City computer must be licensed to the City for that computer.

4.1.2.11.3. Employees may not install any software not provided to them by the Information Technology Department without specific authorization by the Chief Information Officer or designee.

4.1.2.11.4. City employees shall not duplicate, copy, or reproduce any software purchased by and/or licensed to the City, or any related documentation without prior written approval from the Chief Information Officer. City employees shall not give City purchased or licensed software to any non-employees, including, but not limited to clients, contractors, customers, and others without prior written approval from the Chief Information Officer.

4.1.2.11.5. Software and work products (documents, databases, spreadsheets, etc.) developed by employees on City time, or on City owned equipment, or for City projects, shall be the property of the City. Such software and/or work products are for the exclusive use of the City, its officers, agents, and employees. Such software and/or work products may not be sold, transferred, or given to any person without the prior written approval of the City Manager or designee.

4.1.2.11.6. Software must be registered in the name of the City and the Department in which it will be used. Software shall not be registered in an individual employee user's name.

4.1.2.11.7. Game software is an inappropriate use of City equipment and shall not be tolerated. Games discovered during audits shall be eliminated and the employee user may be subject to disciplinary action.

4.1.2.12. Mobile Devices, Cellular Telephones

4.1.2.12.1. Authorized Usage **-** City owned cellular telephones, electronic paging devices, tablets, and other portable or wireless communications devices are intended for City business and

expected to be used for City business. Personal usage related to work assignments (e.g., personal calls which need to be made when away from an office with land line telephones, etc.) and other occasional personal usage is permitted, as long as the personal use is reasonable and prudent.

4.1.2.12.2. Responsibilities of City Managers and Department Heads - The City Manager/Deputy City Manager/Assistant City Manager and/or Department Heads are responsible for:

4.1.2.12.2.1.1. Approving requests for cellular telephones, electronic paging devices, and other wireless communications devices from their respective subordinates;

4.1.2.12.2.1.2. Insuring that requests are in conformance with the procedures outlined herein, or that exceptions are justified;

4.1.2.12.2.1.3. Insuring that all persons assigned a City owned cellular telephone, electronic paging device, and/or other wireless communications device, are provided access to a copy of this Policy and Procedure, and that the individual is in compliance with it;

4.1.2.12.2.1.4. Conducting periodic inventories of cellular telephones, electronic paging devices, and other wireless communications devices within their respective departments to insure accountability;

4.1.2.12.2.1.5. Conducting annual reviews of assigned devices to determine if such assignments continue to be justified; and;

4.1.2.12.2.1.6. Informing appropriate employees responsible for City Communications of all reassignments of cellular telephones, electronic paging devices, and/or other wireless communications devices.

4.1.2.12.3. Responsibilities of Employees - Employees who are assigned the use of City owned cellular telephones, electronic paging devices, and/or other wireless communications devices are responsible for the following:

4.1.2.12.3.1. Insuring the physical security of such devices, including the active use of passcodes, passwords, and prevention of misuse by others

4.1.2.12.3.2. Insuring that all communications on such devices are kept to the briefest duration possible;

4.1.2.12.3.3. Keeping personal communications to a minimum; and

4.1.2.12.3.4. Insuring that any personal use does not detract from the employee’s availability for completion of assigned duties.

4.1.2.12.4. Eligibility Criteria - Employees eligible for assignment of City owned cellular telephones, electronic paging devices, and other wireless communications devices are those designated by the City Manager/Deputy City Manager/Assistant City Manager and/or Department Heads, including (but not limited to):

4.1.2.12.4.1. City Manager's Office staff, Department Heads and employees who are frequently in a vehicle, if the individual must conduct City business by telephone while in the field, and it can be shown that cost savings and customer service efficiency will be realized through use of such devices;

4.1.2.12.4.2. City Manager's Office staff, Department Heads and employees who have a critical need to maintain accessibility with other department managers, city management staff and public officials, in order to insure uninterrupted customer services and /or the integrity of the organization;

4.1.2.12.4.3. Public safety positions and vehicles, to provide immediate and direct telephone communications with citizens, outside agencies cooperating in operations, or other resource entities outside of City government, and to provide for communications which may be inappropriate for mobile radios;

4.1.2.12.4.4. Employees involved in the City's emergency response plan; and

4.1.2.12.4.5. Department Heads and employees who have responsibility for responding to public safety incidents in the field.

4.1.2.12.5. Mobile Device Management – In order to safeguard city property, and to prevent breach and/or loss, the City may install device management software on any or all city-owned mobile devices, to include emergency locators, remote device disable, device wipe, and other functions as deemed necessary by the Chief Information Officer.

4.1.2.12.6. Requests for new data phones must be made directly to the City Manager's Office by the Department Head of the employee requesting the phone. The approving City Manager's Office representative must provide or appropriate budgeted funds to support he additional cost of the phone and data plan. The CIO will be notified upon approval, and the phone will be purchased and provided to the employee.

4.1.3. Security - It is the responsibility of every employee to operate all City telecommunications, computer, or other electronic equipment in such a way as to minimize the risk of unauthorized access to, or loss of, any City resource by any other party, to ensure that City resources are not misused

by any other person, and to act so as to protect the integrity of the data and resources of the City.

4.1.3.1. Password Policy - Each City employee (who uses computers) must have a unique password.

4.1.3.1.1. Passwords may not be written down where they can be found by unauthorized personnel or be shared with other individuals. It is the responsibility of the employee to maintain the secrecy of their passwords.

4.1.3.2. All employees shall immediately report any unauthorized access or unauthorized access attempt, virus infection, spyware infection, or other unauthorized or illegal resource use to the Chief Information Officer or his designee.

4.1.3.3. Employees shall not download or install any software of any kind whatever from the Internet or any storage device or media to any City-owned computer without the prior consent of the Chief Information Officer.

4.1.4. Technology Procurement

4.1.4.1. Departments will coordinate all technology or software related purchase requests (including grant proposals, RFPs, bids, contracts, purchase orders, and City credit card purchases) with the Chief Information Officer or designee verbally or in writing prior to purchase. Once agreed upon, purchases will be submitted to the Assistant City Manager to whom the requesting Department reports for final approval. The purpose of this review is:

- To ensure that the product(s) obtained are compatible with City standards and existing infrastructure
- To avoid unnecessary and costly duplication of capabilities
- To minimize impacts on support personnel
- To ensure all costs are properly considered
- To ensure that the proposed equipment or software does not interfere with the operation of existing systems, or create any undue risk to City resources

4.1.4.2. Departments will involve the IT department in the earliest planning stages of any grant proposal, RFP, bid, contracts, or purchase, etc. which will result in IT related services or products being obtained, prior

to the submission of any request to the purchasing department, or City Council.

4.1.5. Radio System Usage

4.1.5.1. The radio system provided by the City supports many departments, and is mission critical to our Public Safety operations. All users must, at all times, use appropriate communications discipline, handle the equipment with care, and avoid any activity which might reduce the effectiveness of the system for other users.

4.1.5.2. Malfunctions, damage, or loss, of any radio equipment must be immediately reported to Information Technology, to prevent unauthorized access, or disruption of the system.

4.1.5.3. The department to whom a radio has been issued is responsible for all costs associated with damage or loss to individual radios assigned to them.

4.1.5.4. Departments may not operate any system or equipment utilizing radio communications without the express permission of the Chief Information Officer.

4.1.5.5. All frequency assignments requiring FCC authorization must be handled, processed, and maintained by the Information Technology Department, to ensure appropriate coordination of licensing.

Original signed by Dan Johnson on February 20, 2015

_____

Dan Johnson, City Manager

_____

Date