Finalized: Friday, December 3, 2021

ACCEPTABLE USE POLICY

This policy covers the acceptable use of technology (including computer equipment, e-mail, and other technical resources and services) at the City of Boston. It applies to all employees and contractors doing business on behalf of the City.

Technology can play an important role in providing constituents the best and most efficient services. Many City of Boston employees interact with City technology every day, from their boston.gov email account to their City-issued desktop or phone. City-issued equipment remains the property of the City of Boston at all times, so the use of City equipment should be limited to business-related activities and all City technology resources should be used responsibly.

(1) Applicability

(1.1) This policy applies to all employees and affiliates including contractors, consultants, vendors, etc. at the City who are granted access to equipment, software, networks, etc. that is owned, leased, and/or operated/maintained by the City of Boston. These individuals are referred to as "user(s)."

(1.2) By accessing or using a piece of City technology, you are consenting to the policy. Please note that any use of City technology may be monitored.

(1.3) This policy is not meant to cover every form of acceptable and unacceptable use. Users have the responsibility to use the City's technology resources in an efficient, effective, and lawful manner.

(2) Helpful definitions

(2.1) **City technology tools:** any technology tools or devices issued by the City of Boston or used for conducting City business. This includes hardware (e.g. City-issued desktops, laptops, desk phones, cell phones, etc.) and software (any applications used on City devices or owned by the City, including Google Suite – when logged in using your City account – and Microsoft Office).

(2.2) **City technology access:** anything accessed on the City network, which includes the City's employee WiFi network. This also covers the **remote access** of personal

devices accessing the City's network (e.g. if you remote into the City network from a personal computer).

(2.3) **Personal device:** any kind of device not issued by the City that is being used to conduct City business, including phones and laptops.

(3) Policy

(3.1) **Acceptable use of City technology tools:** City of Boston employees should use City technology tools for business purposes and in a way that is consistent with their City job. City technology tools remain the property of the City of Boston at all times. Employees are expected to take reasonable care of the City's technology equipment and should report any damage or theft. Employees are only permitted to use City technology tools for purposes which are safe (pose no risk to employees or assets), legal, and ethical. Employees are expected to complete the annual cyber security training coordinated by the Department of Innovation and Technology (DoIT) to ensure they are aware of how to be secure while using the City's technology tools.

(3.1.1) **Damage or theft**: if an employee's device is damaged, the employee should report the damage to the DoIT Service Desk. The DoIT Service Desk will determine if the damage is covered under any existing warranties. Any costs associated with damaged or stolen equipment should be paid for by the employee's department.

(3.2) **Acceptable use of City technology access:** Access to the City's network is intended for business use by current City employees and other users, such as contractors and vendors, as required. Access is determined at the City's discretion, and the City holds the right to withhold or remove access as needed. Employee departure, termination, and/or suspension will result in loss of access. Employees should take note of any other City policies that may impact their job, including data sharing and social media policies.

(3.2.1) **Remote access:** Any remote personal computer or workstation that initiates a request for remote access must meet the minimum security requirements set by the City. This includes operating system level, service pack, and anti-virus software. If the personal computer does not meet these requirements, access will be denied until the personal computer or workstation has been remediated. The City of Boston is not responsible for

supporting or remediating issues with home or non-City-issued computers, laptops, or workstations.

(3.3) **Acceptable use of City email:** Employees should use their boston.gov email address to conduct City business. Do not use a personal email to conduct City work. Do not use a boston.gov email address to conduct personal business.

(3.3.1) If an employee leaves the City, the employee's manager may request a delegate for the departing employee's Boston.gov email address. The delegate will have access to the department employee's inbox and any items stored on Google Drive.

(3.4) **Acceptable use of personal devices:** No employee is required to use a personal device for City business. However, an employee may use a personal device at their discretion (e.g. connecting City email to a personal cell phone, accessing the City's Google Suite from a personal laptop, remoting into the City network with a personal device, etc.).

(3.4.1) **Security measures:** Any personal devices that are used for City business should have proper security measures with respect to access, transmission, and storage of information. Ensure that the personal device is password protected and locked after 15 minutes of inactivity.

(3.4.1.1) **Personal devices and network access:** personal devices that meet the proper security measures may request VPN (virtual private network) access to remotely access the City's network. Personal devices that meet the proper security measures may use the City's employee WiFi network. However, no employee may directly connect a personal device to the City network (e.g. by using an ethernet cable and plugging a device into a City network jack). Proper security measures are automatically assessed by City appliances during user login.

(3.4.2) **Right to inspect personal devices:** The City of Boston will respect the privacy of personal devices but reserves the right to request access to the device to implement security controls or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings or Freedom of Information Act (FOIA) requests related to City business operations.

(3.5) **Unacceptable Use:** Unless such use is reasonably related to a user's job, it is unacceptable for any person to use City technology or access for:

(3.5.1) the purpose of gambling/gaming or engaging in any illegal activity;

(3.5.2) any commercial purpose;
(3.5.3) any purpose involving a political campaign;
(3.5.4) the transmission of confidential information to unauthorized recipients;
(3.5.5) viewing, downloading, or transmitting sexually explicit, obscene or otherwise pornographic materials;
(3.5.6) the creation or distribution of chain emails, any disruptive or offensive messages, offensive comments about race, gender, disabilities, age, sexual orientation, gender identity or expression, religious beliefs/practices, political beliefs, or material that is in violation of workplace harassment or workplace violence laws or policies;
(3.5.7) infringement of any intellectual property rights;
(3.5.8) disabling any and all antivirus software or other security controls running on or used by the Department of Innovation and Technology;
(3.5.9) significant consumption of City network and system resources for non-business related activities (such as video, audio or downloading large files) or excessive time spent using City technology or access for non-business purposes (e.g. shopping, social networking, sports related sites, et al).

(3.6) **Personal Use:** City technology tools and technology access are provided solely for the conduct of City business. However, the City realizes and is aware of the large role technology (especially the Internet and email) plays in the daily lives of individuals. In this context, the City acknowledges that a limited amount of personal use of City technology tools and technology access is acceptable. This use must not interfere with the user's job responsibilities; it cannot involve any activities expressly prohibited by this or any other City policy; and it should be limited to designated break periods and/or the user's lunch break.

(3.7) **Accountability:** Users are prohibited from anonymous usage of City technology tools and technology access. In practice, this means users must sign in with their uniquely assigned City of Boston User ID before accessing/using City technology. Similarly, "spoofing" or otherwise modifying or obscuring a user's IP Address or any other user's IP Address is prohibited. Circumventing user authentication or security of any host, network, or account is prohibited. Logging into a device using another user's credentials is prohibited.

(3.8) **Passwords:** Responsible password management by employees is critical to the protection of City of Boston technology assets.

(3.8.1) **Confidentiality**: All passwords are to be treated as sensitive, confidential City information and employees are responsible for maintaining the confidentiality of all City of Boston passwords. This concept applies to all passwords, i.e. whether for a user's personally assigned accounts, shared accounts they are authorized to use, or any other password of which they have knowledge. Never share a password over the phone, on an email or chat message, or write it down and store it anywhere in your office (e.g. a sticky note on your desktop). Employees must keep their password private and never ask another employee for their password.

(3.8.2) **Password security**: A "strong" password is one that is difficult to guess because it is of sufficient length and complexity (mix of upper and lower, numeric and special characters). A poorly chosen or "weak" password is easy to guess and may result in the compromise of the City's applications, systems or even the entire network. You may be prompted by a City of Boston application (e.g. GMail) to have a specific number of characters, numericals, or symbols in a password.

(3.8.3) **Password change:** When an employee resets their password they will be required to choose a password that is different from their last password. The application may keep a list of the user's previous passwords (a "password history") and require a new password that is not in the history list.

(3.8.4) **Forgotten passwords:** If an employee forgets their password, they should reset it themselves at Access Boston by using the "forgot password" prompt. For further assistance, employees should contact the DoIT Service Desk.

(3.8.5) **Suspected disclosure of password:** If an employee suspects an account has been accessed by an unauthorized individual, or that a password has been guessed, discovered, or in any way had its confidentiality compromised, then the employee should immediately change their password and report the incident to their IT Support Staff.

(3.9) **Public Records:** All users are advised that their use of City technology resources, including email, may result in the creation of public records. It is the user's responsibility to properly manage and maintain such records. Please see the Archives' records management page for more information about how long employees are required to keep certain categories of records.

(3.10) **Enforcement**

(3.10.1) **Record of activity:** User activity of City technology tools may be logged. Usage may be monitored or researched in the event of suspected improper usage or policy violations.

(3.10.2) **Blocked or restricted access:** User access to specific internet resources, or categories of internet resources, deemed inappropriate or non-compliant with this policy may be blocked or restricted. A particular web site that is deemed "acceptable" for use may still be judged a risk to the City (e.g. it could be hosting malware), in which case it may also be subject to blocking or restriction.

(3.10.3) **Privacy:** Users have no expectation of privacy regarding their use of City technology resources. Log files, audit trails, and other data about user activities may be used for forensic training or research purposes, as evidence in a legal or disciplinary matter, or for troubleshooting.

(3.10.4) **Consequence of policy violation:** Users found to be in violation of this policy may be subject to discipline up to and including termination. The concept of progressive discipline will apply except in serious cases.

(3.10.5) The City of Boston reserves the right to review any City technology usage not covered by this policy and make a case-by-case determination of whether the use is acceptable or unacceptable.

(4) Roles and responsibilities

(4.1) Users are responsible for their own use of City technology. Users are advised to exercise common sense and follow this acceptable use policy when it comes to using City technology in the absence of specific guidance.

(4.2) The Department of Innovation and Technology is responsible for the maintenance of the Acceptable Use Policy.

(5) Related information

(5.1) Terms of Use and Privacy Policy, covering Boston.gov and digital City services
(5.2) City Clerk Archives Division, Records Management
(5.3) Related archived policies:
- Information Technology Resource Use Policy
- Blackberry and personal digital assistant (PDA) policy
- Remote Access Policy
- Password Policy
- Bring your own device policy
- Laptops and other mobile devices policy

Finalized: Friday, December 3, 2021

Mobile device policy - City issued

(6) Support contact

DoIT Service Desk, 617-635-7378, DOITservicedesk@boston.gov

(7) Retention

The City of Boston Department of Innovation & Technology will retain this policy and review it on an annual basis to ensure that it remains effective, complies with internal operational parameters, and meets identified City of Boston business goals and industry best practices.

10.0 Approval List:

Title:	Name:	Date:
Document Owner	Sarah Figalora	April 20, 2021
Quality Assurance Reviewer	Dan Rothman Greg McCarthy Sarah Figalora Carissa Sacchetti	June 15, 2021
Preliminary Approver	Dan Rothman Greg McCarthy	November 22, 2021
Final Approver	Alex Lawrence	December 3, 2021